TSM-16

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of

T. OWADA et al.

Serial No. 09/987,817 Group Art Unit: 2131

Filed: November 16, 2001 Examiner: R. ANANTHANARAYANAN

For: SYSTEM, METHOD AND APPARATUS FOR DISTRIBUTING DIGITAL CONTENTS, INFORMATION PROCESSING APPARATUS AND DIGITAL CONTENT RECORDING MEDIUM

TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

April 29, 2005

Sir:

Submitted herewith is a certified priority document (JP 2000-351511) of a corresponding Japanese patent application for the purpose of claiming foreign priority under 35 U.S.C. § 119. An indication that this document has been safely received would be appreciated.

Respectfully submitted,

Daniel J. Stanger
Registration No. 32,846
Attorney for Applicant(s)

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.
1800 Diagonal Rd., Suite 370
Alexandria, Virginia 22314
(703) 684-1120
Date: April 29, 2005

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年１１月１７日

出願番号
Application Number: 特願２０００－３５１５１１

出願人
Applicant(s): 株式会社日立製作所

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年１１月　９日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

出証番号　出証特２００１－３０９８６８４

【書類名】　特許願

【整理番号】　HK13585000

【提出日】　平成12年11月17日

【あて先】　特許庁長官　殿

【国際特許分類】　G06F　5/00

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

【氏名】　大和田　徹

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

【氏名】　北原　潤

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

【氏名】　朝日　猛

【特許出願人】

【識別番号】　000005108

【氏名又は名称】　株式会社　日立製作所

【代理人】

【識別番号】　100087170

【弁理士】

【氏名又は名称】　富田　和子

【電話番号】　045(316)3711

【手数料の表示】

【予納台帳番号】　012014

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】明細書

【発明の名称】デジタルコンテンツ配布システム、デジタルコンテンツ配布方法、デジタルコンテンツ配布装置、情報処理装置、および、デジタルコンテンツ記録媒体

【特許請求の範囲】

【請求項１】

デジタルコンテンツを配布するデジタルコンテンツ配布装置と、デジタルコンテンツ配布装置から配布されるデジタルコンテンツを出力する情報処理装置とを備えたデジタルコンテンツ配布システムにおいて、

上記デジタルコンテンツ配布装置は、

デジタルコンテンツを蓄積している蓄積手段と、

デジタルコンテンツの一部分に対して、上記情報処理装置と共有する暗号鍵情報を用いて暗号処理を施す暗号処理手段と、

一部分が暗号化されたデジタルコンテンツを上記情報処理装置に配布する配布手段とを備え、

上記情報処理装置は、

上記デジタルコンテンツ配布装置から配布されるデジタルコンテンツを入力する入力手段と、

入力したデジタルコンテンツ中の暗号化部分に対して、上記デジタルコンテンツ配布装置と共有する暗号鍵情報を用いて復号処理を施す復号処理手段と、

暗号化部分を復号後のデジタルコンテンツを出力する出力手段とを備え、

上記デジタルコンテンツ配布装置の暗号処理手段は、

平文時のデジタルコンテンツのフォーマッティング単位を１単位とし、これらの単位の一部の単位を暗号処理の処理対象として、暗号処理を施すことを特徴とするデジタルコンテンツ配布システム。

【請求項２】

デジタルコンテンツを配布するデジタルコンテンツ配布装置と、デジタルコンテンツ配布装置から配布されるデジタルコンテンツを出力する情報処理装置とを備えたデジタルコンテンツ配布システムにおいて、

上記デジタルコンテンツ配布装置は、

上記情報処理装置と共有する暗号鍵情報を用いて一部分が暗号化されたデジタルコンテンツを蓄積している蓄積手段と、

蓄積しているデジタルコンテンツを上記情報処理装置に配布する配布手段とを備え、

上記情報処理装置は、

上記デジタルコンテンツ配布装置から配布されるデジタルコンテンツを入力する入力手段と、

入力したデジタルコンテンツ中の暗号化部分に対して、上記デジタルコンテンツ配布装置と共有する暗号鍵情報を用いて復号処理を施す復号処理手段と、

暗号化部分を復号後のデジタルコンテンツを出力する出力手段とを備え、

上記デジタルコンテンツ配布装置の蓄積手段が蓄積しているデジタルコンテンツは、

平文時のデジタルコンテンツのフォーマッティング単位を１単位とし、これらの単位の一部の単位が暗号化対象となるようにして暗号化されていることを特徴とするデジタルコンテンツ配布システム。

【請求項３】

デジタルコンテンツを配布するデジタルコンテンツ配布装置と、デジタルコンテンツ配布装置から配布されるデジタルコンテンツを出力する情報処理装置とを備えたデジタルコンテンツ配布システムにおいて、上記デジタルコンテンツ配布装置から上記情報処理装置へデジタルコンテンツを配布する方法であって、

上記デジタルコンテンツ配布装置が、上記情報処理装置と共有する暗号鍵情報を用いて一部分が暗号化されたデジタルコンテンツを、上記情報処理装置に配布し、

上記情報処理装置が、上記デジタルコンテンツ配布装置から配布されるデジタルコンテンツ中の暗号化部分に対して、上記暗号鍵情報を用いて復号処理を施し、

上記デジタルコンテンツ配布装置が配布するデジタルコンテンツは、

平文時のデジタルコンテンツのフォーマッティング単位を１単位とし、これら

の単位の一部の単位が暗号化対象となるようにして暗号化されていることを特徴とするデジタルコンテンツ配布方法。

【請求項４】

請求項３記載のデジタルコンテンツ配布方法であって、

平文時のデジタルコンテンツが、ＪＰＥＧ（Joint Photographic Experts Group）方式でフォーマッティングされているＪＰＥＧデータである場合に、

上記ＪＰＥＧデータが暗号化される際には、

８画素×８画素からなる圧縮単位ブロックを１単位とし、一部のブロックが暗号化されることを特徴とするデジタルコンテンツ配布方法。

【請求項５】

請求項３記載のデジタルコンテンツ配布方法であって、

平文時のデジタルコンテンツが、ＪＰＥＧ（Joint Photographic Experts Group）方式でフォーマッティングされているＪＰＥＧデータである場合に、

上記ＪＰＥＧデータが暗号化される際には、

８画素×８画素からなる圧縮単位ブロックを１単位とし、一部または全部のブロックについて、各々、該ブロック内の高周波領域部分または低周波領域部分が暗号化されることを特徴とするデジタルコンテンツ配布方法。

【請求項６】

請求項３記載のデジタルコンテンツ配布方法であって、

平文時のデジタルコンテンツが、ＭＰＥＧ（Moving Picture Experts Group）方式でフォーマッティングされているＭＰＥＧデータである場合には、

上記ＭＰＥＧデータが暗号化される際には、

１フレームを１単位とし、フレーム間の相関性を使わずに圧縮されたフレーム、および、フレーム間の相関性を使って圧縮されたフレームのうちの、いずれか一方について、その全部または一部が暗号化されることを特徴とするデジタルコンテンツ配布方法。

【請求項７】

請求項３記載のデジタルコンテンツ配布方法であって、

平文時のデジタルコンテンツが、周波数成分ごとにサンプリングして個別に符

号化された音声データである場合には、

上記音声データが暗号化される際には、

符号化単位サンプルを１単位とし、高周波成分のサンプルまたは低周波成分のサンプルが暗号化されることを特徴とするデジタルコンテンツ配布方法。

【請求項８】

デジタルコンテンツを蓄積している蓄積手段と、

デジタルコンテンツの一部分に対して、該デジタルコンテンツの配布先の情報処理装置と共有する暗号鍵情報を用いて暗号処理を施す暗号処理手段と、

一部分が暗号化されたデジタルコンテンツを上記情報処理装置に配布する配布手段とを備え、

上記暗号処理手段は、

平文時のデジタルコンテンツのフォーマッティング単位を１単位とし、これらの単位中の一部の単位を暗号処理の処理対象として、暗号処理を施すことを特徴とするデジタルコンテンツ配布装置。

【請求項９】

配布先の情報処理装置と共有する暗号鍵情報を用いて一部分が暗号化されたデジタルコンテンツを蓄積している蓄積手段と、

蓄積しているデジタルコンテンツを上記情報処理装置に配布する配布手段とを備え、

上記蓄積手段が蓄積しているデジタルコンテンツは、

平文時のデジタルコンテンツのフォーマッティング単位を１単位とし、これらの単位の一部の単位が暗号化対象となるようにして暗号化されていることを特徴とするデジタルコンテンツ配布装置。

【請求項１０】

請求項８または８記載のデジタルコンテンツ配布装置であって、

平文時のデジタルコンテンツが、ＪＰＥＧ（Joint Photographic Experts Group）方式でフォーマッティングされているＪＰＥＧデータである場合に、

上記ＪＰＥＧデータが暗号化される際には、

８画素×８画素からなる圧縮単位ブロックを１単位とし、一部のブロックが暗

号化されることを特徴とするデジタルコンテンツ配布装置。

【請求項１１】

請求項８または９記載のデジタルコンテンツ配布装置であって、

平文時のデジタルコンテンツが、ＪＰＥＧ（Joint Photographic Experts Group）方式でフォーマッティングされているＪＰＥＧデータである場合に、

上記ＪＰＥＧデータが暗号化される際には、

８画素×８画素からなる圧縮単位ブロックを１単位とし、一部または全部のブロックについて、各々、該ブロック内の高周波領域部分または低周波領域部分が暗号化されることを特徴とするデジタルコンテンツ配布装置。

【請求項１２】

請求項８または９記載のデジタルコンテンツ配布装置であって、

平文時のデジタルコンテンツが、ＭＰＥＧ（Moving Picture Experts Group）方式でフォーマッティングされているＭＰＥＧデータである場合に、

上記ＭＰＥＧデータが暗号化される際には、

１フレームを１単位とし、フレーム間の相関性を使わずに圧縮されたフレーム、および、フレーム間の相関性を使って圧縮されたフレームのうちの、いずれか一方について、その全部または一部が暗号化されることを特徴とするデジタルコンテンツ配布装置。

【請求項１３】

請求項８，９，１０，１１または１２記載のデジタルコンテンツ配布装置から配布されるデジタルコンテンツを出力する情報処理装置であって、

上記デジタルコンテンツ配布装置から配布されるデジタルコンテンツを入力する入力手段と、

入力したデジタルコンテンツ中の暗号化部分に対して、上記デジタルコンテンツ配布装置と共有する暗号鍵情報を用いて復号処理を施す復号処理手段と、

暗号化部分を復号後のデジタルコンテンツを出力する出力手段とを備えたことを特徴とする情報処理装置。

【請求項１４】

平文時のデジタルコンテンツのフォーマッティング単位を１単位とし、これら

の単位中の一部の単位が暗号化対象となるようにして暗号化されたデジタルコンテンツが記録されていることを特徴とするデジタルコンテンツ記録媒体。

【請求項１５】

請求項１４記載のデジタルコンテンツ記録媒体であって、

平文時のデジタルコンテンツが、ＪＰＥＧ（Joint Photographic Experts Group）方式でフォーマッティングされているＪＰＥＧデータである場合に、

上記ＪＰＥＧデータが暗号化される際には、

８画素×８画素からなる圧縮単位ブロックを１単位とし、一部のブロックが暗号化されることを特徴とするデジタルコンテンツ記録媒体。

【請求項１６】

請求項１４記載のデジタルコンテンツ記録媒体であって、

平文時のデジタルコンテンツが、ＪＰＥＧ（Joint Photographic Experts Group）方式でフォーマッティングされているＪＰＥＧデータである場合に、

上記ＪＰＥＧデータが暗号化される際には、

８画素×８画素からなる圧縮単位ブロックを１単位とし、一部または全部のブロックについて、各々、該ブロック内の高周波領域部分または低周波領域部分が暗号化されることを特徴とするデジタルコンテンツ記録媒体。

【請求項１７】

請求項１４記載のデジタルコンテンツ記録媒体であって、

平文時のデジタルコンテンツが、ＭＰＥＧ（Moving Picture Experts Group）方式でフォーマッティングされているＭＰＥＧデータである場合に、

上記ＭＰＥＧデータが暗号化される際には、

１フレームを１単位とし、フレーム間の相関性を使わずに圧縮されたフレーム、および、フレーム間の相関性を使って圧縮されたフレームのうちの、いずれか一方について、その全部または一部が暗号化されることを特徴とするデジタルコンテンツ記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、著作権保護が必要なデジタルコンテンツを扱う技術に関し、特に、複製による不正使用を防ぎ、かつ、正当な使用権利を持たないユーザの視聴覚欲求を刺激する形での利用を可能としながら、デジタルコンテンツを配布し、配布先の情報処理装置で出力する方法に関する。

【０００２】

【従来の技術】

近年、映像や音声などの高付加価値な情報をデジタル形式で配布する要求が高まっており、デジタルコンテンツの著作権保護を図るために、不正コピーの防止が重要視されてきている。すなわち、デジタルコンテンツは、容易にコピーできる上、コピーしても品質が劣化しないので、既に不正コピーによる著作権の侵害等の弊害が生じてきている。

【０００３】

コピー防止手段の１つとしては、一般に、デジタルコンテンツの暗号化が用いられており、正当な暗号鍵情報を入手したユーザのみが、暗号化されたデジタルコンテンツを復号し、その中身を確かめることができるようにしている。

【０００４】

【発明が解決しようとする課題】

しかしながら、デジタルコンテンツを単純に暗号化した場合、暗号化されたデジタルコンテンツは、正当な暗号鍵情報がないと全く視聴することができなくなってしまう。

【０００５】

これは、デジタルコンテンツが何らかのフォーマットに従ってフォーマッティングされているにも関わらず、フォーマットを無視した単純な暗号化が行われることにより、デジタルコンテンツのデータ構造が破壊されてしまい、デジタルコンテンツを再生するソフトウェアやハードウェアがデータ構造を全く解釈できなくなるからである。

【０００６】

そこで、ユーザは、デジタルコンテンツを購入するなどして、正当な暗号鍵情報を入手しない限り、その中身を確かめることができず、ユーザにとってはデジ

タルコンテンツ購入の敷居が高くなってしまう。

【０００７】

本発明の目的は、デジタルコンテンツの権利を保護すると共に、ユーザの視聴覚欲求を刺激することにより、デジタルコンテンツの配布または販売を促進するデジタルコンテンツ配布システム等を提供することにある。

【０００８】

【課題を解決するための手段】

上記目的を達成するために、本発明は、デジタルコンテンツを配布するデジタルコンテンツ配布装置と、デジタルコンテンツ配布装置から配布されるデジタルコンテンツを出力する情報処理装置とを備えたデジタルコンテンツ配布システムにおいて、上記デジタルコンテンツ配布装置が、上記情報処理装置と共有する暗号鍵情報を用いて一部分が暗号化されたデジタルコンテンツを、上記情報処理装置に配布し、上記情報処理装置が、上記デジタルコンテンツ配布装置から配布されるデジタルコンテンツ中の暗号化部分に対して、上記暗号鍵情報を用いて復号処理を施すようにしている。

【０００９】

そして、特に、本発明では、上記デジタルコンテンツ配布装置から配布されるデジタルコンテンツが、平文時のデジタルコンテンツのフォーマッティング単位を１単位とし、これらの単位中の一部の単位が暗号化対象となるようにして暗号化されたものであるようにしている。

【００１０】

【発明の実施の形態】

以下、本発明の実施の形態について図面を参照して説明する。

【００１１】

図１は、本実施形態に係るデジタルコンテンツ配布システムの概略構成図である。

【００１２】

図中、１００はデジタルコンテンツ配布装置、１０１は情報処理装置、１０２は情報処理装置本体、１０３は表示装置である。

【００１３】

本実施形態に係るデジタルコンテンツ配布システムは、デジタルコンテンツ配布装置１００によってデジタルデータとして配布される高付加価値コンテンツの権利保護を大前提としている。すなわち、本実施形態に係るデジタルコンテンツ配布システムは、デジタルコンテンツ配布装置１００と情報処理装置本体１０２との間を転送されるデジタルコンテンツ（配布データ）、および、情報処理装置本体１０２と表示装置１０３との間を転送されるデジタルコンテンツ（表示データ）が、各々、デジタルデータであるようなものを対象にしており、これらを暗号化することで保護を図っている。

【００１４】

そして、本実施形態に係るデジタルコンテンツ配布システムは、ユーザの視聴覚欲求を刺激する形でデジタルコンテンツを配布可能とすることを目的としている。すなわち、本実施形態に係るデジタルコンテンツ配布システムは、暗号化されたデジタルコンテンツで、ユーザの視聴覚要求を刺激することを可能とするものである。

【００１５】

具体的には、デジタルコンテンツ配布装置１００と情報処理装置本体１０２との間を転送されるデジタルコンテンツは、例えば、ＪＰＥＧ（Joint Photographic Experts Group）やＭＰＥＧ（Moving Picture Experts Group）などの、予め決められた圧縮方式でフォーマッティングされたデジタルデータが、例えば、ＤＥＳ（Data Encryption Standard）などの、予め決められた暗号方式で暗号化された暗号化データである。

【００１６】

ここで、デジタルコンテンツ配布装置１００は、ネットワークを経由してデジタルコンテンツを配布するネットワーク装置であっても、例えば、光ディスク媒体や磁気ディスク媒体などの、デジタルコンテンツが記録された記録媒体であってもよい。

【００１７】

すなわち、デジタルコンテンツ配布装置１００によって配布されるデジタルコ

ンテンツは、デジタルコンテンツ配布装置１００から配布される時点で暗号化されていればよく、暗号処理を施すのがデジタルコンテンツ配布装置１００でなくてもよい。

【００１８】

さて、図１に示すように、本実施形態に係るデジタルコンテンツ配布システムにおいては、デジタルコンテンツ配布装置１００および情報処理装置本体１０２は、何らかの方法によって、デジタルコンテンツ（配布データ）を暗号化／復号化するための暗号鍵情報１０４を共有する機能を有している。

【００１９】

暗号鍵情報１０４を共有する方法については、様々な方法が公知技術となっており、どのような方法を採用してもよい。

【００２０】

例えば、デジタルコンテンツの暗号化に用いられた暗号鍵情報１０４を管理しているネットワーク装置から、情報処理装置本体１０２が暗号鍵情報１０４を入手するという方法が挙げられる。このとき、ネットワーク装置が、情報処理装置本体１０２の公開鍵情報を用いて暗号鍵情報１０４を暗号化し、情報処理装置本体１０２が、自身の秘密鍵情報で復号するようにする。

【００２１】

また、例えば、磁気ディスク媒体に記録されているデジタルコンテンツ（暗号化済み）の暗号化に用いられた暗号鍵情報１０４を、情報処理装置本体１０２の製造時に、情報処理装置本体１０２の内部の不揮発性記憶装置に記録しておくという方法が挙げられる。

【００２２】

同様に、図１に示すように、本実施形態に係るデジタルコンテンツ配布システムにおいては、情報処理装置本体１０２および表示装置１０３は、何らかの方法によって、デジタルコンテンツ（表示データ）を暗号化／復号化するための暗号鍵情報１０５を共有する機能を有している。

【００２３】

暗号鍵情報１０５を共有する方法についても、暗号鍵情報１０４を共有する方

法と同様に、様々な方法が公知技術となっており、どのような方法を採用してもよい。

【００２４】

例えば、情報処理装置本体１０２がデジタルコンテンツの暗号化に用いた暗号鍵情報１０５を、表示装置１０３が情報処理装置本体１０２から入手するという方法が挙げられる。このとき、情報処理装置本体１０２が、表示装置１０３の公開鍵情報を用いて暗号鍵情報１０５を暗号化し、表示装置１０３が、自身の秘密鍵情報で復号するようにする。

【００２５】

また、例えば、暗号鍵情報１０５を、情報処理装置本体１０２および表示装置１０３の製造時に、各々の内部の不揮発性記憶装置に記録しておくという方法が挙げられる。

【００２６】

また、図１に示すように、本実施形態に係るデジタルコンテンツ配布システムにおいては、情報処理装置本体１０２は、

（１）デジタルコンテンツ配布装置１００から配布されるデジタルコンテンツ中の暗号化部分に対して、暗号鍵情報１０４を用いて復号処理１０６を施す復号機能、

（２）暗号化部分を復号後のデジタルコンテンツの展開処理１０７を行う展開機能、

（３）展開したデジタルコンテンツを、表示装置１０３が要求するビットレートで出力するための表示データに変換する表示制御処理１０８を行う表示制御機能、

（４）表示データの一部分に対して、暗号鍵情報１０５を用いて暗号処理１０９を施す暗号機能、

を有している。

【００２７】

また、図１に示すように、本実施形態に係るデジタルコンテンツ配布システムにおいては、表示装置１０３は、

（１）情報処理装置本体１０２の暗号機能によって暗号化された表示データ中の暗号化部分に対して、暗号鍵情報１０５を用いて復号処理１１０を施す復号機能、

（２）暗号化部分を復号後の表示データの表示処理１１１を行う表示機能、

を有している。

【００２８】

次に、本実施形態に係るデジタルコンテンツ配布システムの概略動作について、図２を用いて説明する。

【００２９】

図２は、本実施形態に係るデジタルコンテンツ配布システムの概略動作フローチャートである。

【００３０】

図２において、まず、デジタルコンテンツ配布装置１００および情報処理装置本体１０２は、何らかの方法によって、デジタルコンテンツ（配布データ）を暗号化／復号化するための暗号鍵情報１０４を共有する（ステップ２０１）。上述したように、暗号鍵情報１０４を共有する方法については、様々な方法が公知技術となっており、どのような方法を採用してもよいので、ここでは規定しない。

【００３１】

続いて、デジタルコンテンツ配布装置１００は、情報処理装置本体１０２へ、暗号鍵情報１０４を用いて一部分が暗号化されたデジタルコンテンツを配布する（ステップ２０２）。上述したように、デジタルコンテンツ配布装置１００によって配布されるデジタルコンテンツは、デジタルコンテンツ配布装置１００から配布される時点で暗号化されていればよく、暗号処理を施すのがデジタルコンテンツ配布装置１００でなくてもよい。

【００３２】

続いて、情報処理装置本体１０２は、デジタルコンテンツ配布装置１００から配布されたデジタルコンテンツ中の暗号化部分に対して、暗号鍵情報１０４を用いて復号処理１０６を施す（ステップ２０３）。ステップ２０３の処理によって、情報処理装置本体１０２は、その内部に、平文のデジタルコンテンツを得るこ

ととなる。

【００３３】

続いて、情報処理装置本体１０２は、ステップ２０３の処理で得られたデジタルコンテンツの展開処理１０７を行う（ステップ２０４）。例えば、ステップ２０３の処理で得られたデジタルコンテンツがＭＰＥＧ方式でフォーマッティングされているＭＰＥＧデータである場合には、ステップ２０４の処理によって、情報処理装置本体１０２は、その内部に、毎秒３０フレームからなる動画像データを得ることとなる。

【００３４】

続いて、ステップ２０４の処理で得られた動画像データを含む表示データに対して、表示装置１０３が要求するビットレートで出力するための表示制御処理１０８を行う（ステップ２０５）。例えば、表示装置１０３がＴＦＴ（Thin Film Transistor）液晶表示装置の場合は、ステップ２０５の処理では、情報処理装置本体１０２は、毎秒６０～７０フレーム程度のシーケンシャルな表示データを生成する。

【００３５】

続いて、情報処理装置本体１０２および表示装置１０３は、何らかの方法によって、デジタルコンテンツ（表示データ）を暗号化／復号化するための暗号鍵情報１０５を共有する（ステップ２０６）。上述したように、暗号鍵情報１０５を共有する方法については、様々な方法が公知技術となっており、どのような方法を採用してもよいので、ここでは規定しない。

【００３６】

続いて、情報処理装置本体１０２は、ステップ２０５の処理で生成した表示データ中の一部分に対して、暗号鍵情報１０５を用いて暗号処理１０９を施す（ステップ２０７）。ステップ２０７の処理によって、情報処理装置本体１０２は、その内部に、一部分が暗号化された表示データを得ることとなる。

【００３７】

続いて、情報処理装置本体１０２は、表示装置１０３へ、一部分が暗号化された表示データを出力する（ステップ２０８）。

【００３８】

続いて、表示装置１０３は、情報処理装置本体１０２から出力された表示データ中の暗号化部分に対して、暗号鍵情報１０５を用いて復号処理１１０を施す（ステップ２０９）。ステップ２０９の処理によって、表示装置１０３は、その内部に、平文の表示データを得ることとなる。

【００３９】

続いて、表示装置１０３は、ステップ２０９の処理によって得られた表示データの表示処理１１１を行う（ステップ２１０）。ステップ２１０の処理によって、ステップ２０４の処理によって得られた動画像データを含む表示データが表示されることとなる。

【００４０】

以上、ステップ２０１～ステップ２１０の処理によって、デジタルコンテンツ配布装置１００から配布されるデジタルコンテンツが、表示装置１０３で表示されることとなる。

【００４１】

なお、以下では、本実施形態に係るデジタルコンテンツ配布システムの動作のうち、ステップ２０１～ステップ２０４の処理によって実現される動作を、「配布経路暗号化」動作と称し、ステップ２０５～ステップ２１０の処理によって実現される動作を、「出力経路暗号化」動作と称する。

【００４２】

また、ステップ２０６の処理は、配布経路暗号化動作に先立って行われても、並行して行われてもよい。また、ステップ２０５，ステップ２０６，ステップ２０７の処理は、情報処理装置１０１の構成によっては順番が逆転してもよい。

【００４３】

次に、配布経路暗号化動作の詳細について説明する。

【００４４】

まず、本実施形態に係る情報処理装置１０１の概略動作について、図３を用いて説明する。

【００４５】

図３は、本実施形態に係る情報処理装置１０１の概略構成図である。

【００４６】

図３では、パーソナルコンピュータ（ＰＣ）などの情報処理装置１０１のうち、表示に関する部分であって、かつ、配布経路暗号化動作に関する部分のみを示している。

【００４７】

図中、１０２は情報処理装置本体、１０３は表示装置、１０４は暗号鍵情報、３０１は中央演算装置（ＣＰＵ：Central Processing Unit）、３０２はシステムメモリ、３０３は表示制御装置、３０４は表示メモリ、３０５は入力制御装置、３０６は通信制御装置、３０７はバス、３０８は復号処理部、３０９はコンテンツ展開処理部である。

【００４８】

図３において、デジタルコンテンツ配布装置１００がネットワーク装置である場合には、通信制御装置３０６が、ＣＰＵ３０１の指示に従って、デジタルコンテンツを入力する。また、デジタルコンテンツ配布装置１００が記録媒体である場合には、入力制御装置３０５が、ＣＰＵ３０１の指示に従って、デジタルコンテンツを入力する。通信制御装置３０６または入力制御装置３０５が入力したデジタルコンテンツは、ＣＰＵ３０１の指示に従って、バス３０７を介して表示制御装置３０３に入力される。

【００４９】

表示制御装置３０３においては、復号処理部３０８が、入力したデジタルコンテンツ中の暗号化部分に対して、表示制御装置３０３の内部に保持されている暗号鍵情報１０４を用いて復号処理１０６を施し、表示制御装置３０３の内部に、平文のデジタルコンテンツを得る。続いて、コンテンツ展開処理部３０９が、復号処理部３０８が復号したデジタルコンテンツの展開処理１０７を行い、表示制御装置３０３の内部に、展開されたデジタルコンテンツを得る。

【００５０】

ここまでの動作が配布経路暗号化動作に相当している。その後の出力経路暗号化動作の詳細については後述する。

【００５１】

なお、復号処理部３０８およびコンテンツ展開処理部３０９は、表示制御装置３０３内にハードウェアとして実装されるようにしてもよいし、また、表示制御装置３０３内に独自のＣＰＵおよびメモリを設け、ソフトウェアとして実装されるようにしてもよい。

【００５２】

次に、配布経路暗号化動作で、デジタルコンテンツ配布装置１００から配布されるデジタルコンテンツの暗号化方法の一例について、図５および図６を用いて説明する。

【００５３】

図５は、デジタルコンテンツ配布装置１００から配布されるデジタルコンテンツの暗号化方法の一例を示す説明図であり、図６は、図５に示す暗号化方法で暗号化されたデジタルコンテンツを表示装置１０３で表示した場合の表示イメージを示す説明図である。

【００５４】

図５および図６では、デジタルコンテンツがＭＰＥＧデータである場合を例にしている。

【００５５】

ＭＰＥＧ方式による圧縮では、例えば、１フレームｍ×ｎ画素，毎秒ｋフレームから構成される動画像データは、Ｉピクチャ形式，Ｐピクチャ形式，Ｂピクチャ形式の３つの形式に分類される。

【００５６】

（１）Ｉピクチャ形式

Ｉピクチャ形式では、１フレームｍ×ｎ画素の画像データは、８×８画素の複数のブロックに分割され、各ブロックごとに直交変換処理が施されて周波数領域データに変換された後、量子化されてデータ圧縮が行われる。Ｉピクチャデータでは、元フレーム内のデータのみを対象にした符号化がなされており、Ｉピクチャデータからは、展開処理によって１枚のフレームデータが得られる。

【００５７】

（２）Ｐピクチャ形式

Ｐピクチャ形式では、順方向のフレーム間予測を行ったデータ圧縮が行われる。Ｐピクチャデータでは、Ｉピクチャとの差分情報を用いた符号化がなされており、元フレームの復元には、Ｐピクチャデータ，元画となるＩピクチャデータが必要となる。すなわち、Ｐピクチャデータのみでは画像データは得られない。

【００５８】

（３）Ｂピクチャ形式

Ｂピクチャ形式では、双方向のフレーム間予測を行ったデータ圧縮が行われる。Ｂピクチャデータでは、ＩピクチャとＰピクチャとの間の差分情報を用いた符号化がなされており、元フレームの復元には、Ｐピクチャデータ、元画となるＩピクチャデータ，Ｂピクチャデータが必要となる。すなわち、Ｂピクチャデータのみでは画像データは得られない。

【００５９】

また、１ピクチャデータの符号割り当て量は、図５に示すように、Ｉピクチャ，Ｐピクチャ，Ｂピクチャの順に小さくなる。動画像データは、フレームごとに、例えば、ＩＢＢ，ＰＢＢ，ＰＢＢ，ＩＢＢ，ＰＢＢ，ＰＢＢなどの順番に符号化される。

【００６０】

このような性質を持ったＭＰＥＧデータの暗号化方法としては、以下の３つの方法が考えられる。

【００６１】

（１）第１の暗号化方法

第１の暗号化方法としては、Ｉピクチャデータのみを暗号化するという方法がある。第１の暗号化方法は、さらに、圧縮単位となるブロックごとに暗号化を施す／施さないという方法、および、圧縮単位となるブロック内の周波数成分に着目し、高周波領域データ／低周波領域データごとに暗号化を施す／施さないという方法に分けられる。

【００６２】

まず、前者の方法（圧縮単位となるブロックごとに暗号化を施す／施さないと

いう方法）について説明すると、例えば、図６（ａ）に示す元画像に対して、本方法による暗号化を行う際には、ブロックを暗号処理の処理対象とし、あるブロックには暗号処理を施し、あるブロックには暗号処理を施さないようにする。

【００６３】

本方法により暗号化されたＭＰＥＧデータは、暗号鍵情報１０４を用いた復号処理を施さなければ、表示装置１０３に表示される際のイメージは、図６（ｂ）に示すようになる。本方法では、暗号化を施すブロック数を増減させることで、元画像の汚損度合を制御可能であり、どの程度の開示を行うかを自由に変更することができる。

【００６４】

次に、後者の方法（高周波領域データ／低周波領域データごとに暗号化を施す／施さないという方法）について説明すると、例えば、図６（ａ）に示す元画像に対して、本方法による暗号化を行う際には、ブロック内の低周波領域データを暗号処理の処理対象とし、各ブロック中の低周波領域データには暗号処理を施し、高周波領域データには暗号処理を施さないようにする。本方法により暗号化されたＭＰＥＧデータは、暗号鍵情報１０４を用いた復号処理を施さなければ、表示装置１０３に表示される際のイメージは、図６（ｃ）に示すようになる。

【００６５】

低周波数領域データを暗号化すると、図６（ｃ）に示すように、元画像は大きく汚染され、元画像を観測するのは困難となるが、高周波数領域データを暗号化すると、図示していないが、元画像にノイズが重畳されたイメージとなる。

【００６６】

本方法では、暗号化を施す周波数領域を選択することで、元画像の汚損度合を制御可能であり、どの程度の開示を行うかを自由に変更することができる。また、全てのブロックを暗号処理の処理対象としなくても、一部のブロックを暗号処理の処理対象としてもよい。

【００６７】

第１の暗号化方法によってＩピクチャデータのみを暗号化した場合、暗号鍵情報１０４がないとＩピクチャデータを復元することができず、従って、図５に示

すように、Ｉピクチャデータの差分情報であるＰピクチャデータおよびＢピクチャデータも、暗号化されてはいないが、これらを展開することも不可能となる。例えば、ＩＢＢ，ＰＢＢ，ＰＢＢ，ＩＢＢ，ＰＢＢ，ＰＢＢの順番に符号化された動画像データは、暗号鍵情報１０４がない場合には、×××，×××，×××，×××，×××，×××（×は正常な復号・展開の失敗を意味する。）となって、全てのフレーム共に正常な元画像が得られない。

【００６８】

（２）第２の暗号化方法

第２の暗号化方法としては、Ｐピクチャデータのみを暗号化するという方法がある。第２の暗号化方法も、第１の暗号化方法と同様に、さらに、圧縮単位となるブロックごとに暗号化を施す／施さないという方法、および、圧縮単位となるブロック内の周波数成分に着目し、高周波領域データ／低周波領域データごとに暗号化を施す／施さないという方法に分けられる。

【００６９】

第２の暗号化方法によってＰピクチャデータのみを暗号化した場合、暗号鍵情報１０４がないとＰピクチャデータを復元することができず、従って、図５に示すように、Ｉピクチャデータ，Ｐピクチャデータの差分情報であるＢピクチャデータも、暗号化されてはいないが、これを展開することも不可能となる。例えば、ＩＢＢ，ＰＢＢ，ＰＢＢ，ＩＢＢ，ＰＢＢ，ＰＢＢの順番に符号化された動画像データは、暗号鍵情報１０４がない場合には、Ｉ××，×××，×××，Ｉ××，×××，×××（×は正常な復号・展開の失敗を意味する。）となって、得られる正常な画像フレームはＩピクチャデータのみとなる。

【００７０】

（３）第３の暗号化方法

第３の暗号化方法としては、Ｂピクチャデータのみを暗号化するという方法がある。第３の暗号化方法も、第１の暗号化方法と同様に、さらに、圧縮単位となるブロックごとに暗号化を施す／施さないという方法、および、圧縮単位となるブロック内の周波数成分に着目し、高周波領域データ／低周波領域データごとに暗号化を施す／施さないという方法に分けられる。

【００７１】

第３の暗号化方法によってＢピクチャデータのみを暗号化した場合、図５に示すように、暗号鍵情報１０４がないとＢピクチャデータを復元することができない。例えば、ＩＢＢ，ＰＢＢ，ＰＢＢ，ＩＢＢ，ＰＢＢ，ＰＢＢの順番に符号化された動画像データは、暗号鍵情報１０４がない場合には、Ｉ××，Ｐ××，Ｐ××，Ｉ××，Ｐ××，Ｐ××（Ｘは正常な復号・展開の失敗を意味する。）となって、得られる正常な画像フレームはＩピクチャデータおよびＰピクチャのみとなる。

【００７２】

以上、ＭＰＥＧデータの暗号化方法として３つの方法を説明したが、これらの方法を任意に組み合わせるようにしてもよい。

【００７３】

本実施形態に係るデジタルコンテンツ配布システムによれば、配布経路暗号化動作において、デジタルコンテンツを単純に暗号化するのではなく、暗号処理の処理対象とするデータを選択し、一部分のみを暗号化するようにしているので、正当な暗号鍵情報１０４を有していない場合には、元画像の一部分が汚損した状態となる。一部分が汚損されたデジタルコンテンツは、その価値が損なわれるので、デジタルコンテンツの不正コピーを防止することが可能となり、また、デジタルコンテンツの一部分が開示されるので、ユーザの視聴要求を刺激し、デジタルコンテンツの完全な視聴を促すことが可能となる。

【００７４】

特に、本実施形態に係るデジタルコンテンツ配布システムにおいては、暗号処理の処理対象とするデータを選択する際に、そのフォーマットに着目するようにしている。すなわち、デジタルコンテンツを単なるビット列として暗号処理の処理対象とした場合、ヘッダ，ペイロード，フッタと言ったデータ構造が全て失われてしまい、デジタルコンテンツとして利用することがまったく不可能となってしまうが、本実施形態に係るデジタルコンテンツ配布システムにおいては、デジタルコンテンツを単なるビット列として扱うのではなく、暗号処理の処理対象とするデータを、フォーマットの有意味部分に合わせて選択するようにしているの

で、データ全体ではなく、一部分だけの汚損が可能となっている。

【００７５】

また、本実施形態に係るデジタルコンテンツ配布システムによれば、配布経路暗号化動作において、データ汚損に、暗号鍵情報１０４を用いた暗号処理を利用していることから、ユーザの視聴欲求を刺激するために、完全なデジタルコンテンツとは別に汚損デジタルコンテンツを用意する必要がなく、デジタルコンテンツの配布・蓄積に掛かるコストを低減することが可能となる。

【００７６】

さらに、本実施形態に係るデジタルコンテンツ配布システムによれば、配布経路暗号化動作において、デジタルコンテンツの一部分だけを暗号処理の処理対象とし、デジタルコンテンツ全体に対する暗号処理を避けることによって、暗号処理／復号処理の処理量の軽減も可能となっている。なお、汚損度と処理量とはトレードオフの関係にあり、要求に応じて優先度の変更が容易に可能である。

【００７７】

以上説明したように、本実施形態に係るデジタルコンテンツ配布システムによれば、配布経路暗号化動作によって、デジタルコンテンツの配布経路上で著作権を保護しつつ、ユーザの視聴欲求を刺激することが可能となる。

【００７８】

なお、本実施形態に係る情報処理装置１０１は、図３に示す構成ではなく、図７に示す構成にし、図３に示した復号処理部３０８およびコンテンツ展開処理部３０９を、ソフトウェアで実現するようにしてもよい。

【００７９】

図７は、本実施形態に係る情報処理装置１０１の他の概略構成図である。

【００８０】

図７でも、図３と同様に、ＰＣなどの情報処理装置１０１のうち、表示に関する部分であって、かつ、配布経路暗号化動作に関する部分のみを示している。

【００８１】

図中、図３と同じ構成要素には同じ符号を付与してある。７０１は不揮発性記憶装置である。

【００８２】

図７に示す構成の情報処理装置１０１においては、図３に示した復号処理部３０８およびコンテンツ展開処理部３０９の動作を、ＣＰＵ３０１がシステムメモリ３０２上にプログラムをロードして実行することで実現するものである。

【００８３】

図７において、デジタルコンテンツ配布装置１００がネットワーク装置である場合には、通信制御装置３０６が、ＣＰＵ３０１の指示に従って、デジタルコンテンツを入力する。また、デジタルコンテンツ配布装置１００が記録媒体である場合には、入力制御装置３０５が、ＣＰＵ３０１の指示に従って、デジタルコンテンツを入力する。通信制御装置３０６または入力制御装置３０５が入力したデジタルコンテンツは、ＣＰＵ３０１の指示に従って、バス３０７を介してシステムメモリ３０２に入力される。

【００８４】

ＣＰＵ３０１は、入力したデジタルコンテンツ中の暗号化部分に対して、暗号鍵情報１０４を用いて復号処理１０６を施し、システムメモリ３０２上に、平文のデジタルコンテンツを得る。続いて、ＣＰＵ３０１は、復号したデジタルコンテンツの展開処理１０７を行い、展開されたデジタルコンテンツを得る。得られたデジタルコンテンツは表示制御装置３０３に入力される。

【００８５】

ここで、暗号鍵情報１０４は、図３を用いた説明では、表示制御装置３０３の内部に保持されているものとしたが、図７に示す構成の情報処理装置１０１においては、暗号鍵情報１０４は、不揮発性記憶装置７０１に保持されているものとする。

【００８６】

また、本実施形態に係る情報処理装置１０１は、図３および図７のいずれにおいても、情報処理装置１０２本体と表示装置１０３とを備えた構成としているが、情報処理装置本体１０２と表示装置１０３が一体化した構成であってもよい。すなわち、本実施形態に係る情報処理装置１０１を、いわゆるＰＤＡ（Personal Digital Assistant）などと呼ばれる携帯情報端末としてもよい。

【００８７】

一般に、携帯情報端末は、比較的性能の低いＣＰＵや小容量のメモリなどを用いて構成されることが多いので、比較的重い処理である暗号処理は携帯情報端末にとって大きな負担になるという問題がある。

【００８８】

そこで、このような問題がある携帯情報端末を、本実施形態に係るデジタルコンテンツ配布システムで用いるようにすれば、全体ではなく一部分が暗号化されたデジタルコンテンツを扱うことにより、本発明が目的とする、著作権保護とユーザの視聴覚欲求刺激の両立を実現することができる上、暗号処理量の低減による負荷低下効果を得ることができる。特に、携帯情報端末が暗号処理をソフトウェアで実現する場合には、暗号処理用に高性能なＣＰＵや大容量メモリを搭載する必要がなくなり、低コスト化，低消費電力化といった効果が得られる。また、携帯情報端末が暗号処理専用のハードウェアを備えるようにする場合には、暗号処理専用のハードウェアに必要な処理速度が低下することから、低動作速度による低消費電力化，ハードウェア論理の小規模化による低コスト化といった効果が得られる。

【００８９】

ところで、上述の説明では、ＭＰＥＧデータ（動画像データ）を例にしたが、必ずしも動画像データのみを対象としている訳ではない。

【００９０】

例えば、デジタルコンテンツがＪＰＥＧデータ（静止画像データ）である場合には、上述したＩピクチャデータの暗号化方法と同様の暗号化方法を用いることが可能である。

【００９１】

また、例えば、デジタルコンテンツがＭＰＥＧデータ（音声データ）である場合には、音声情報に対して帯域分割を施し、分割された周波数成分ごとに独立した符号化を行っていることから、低周波成分のみに対する暗号化／高周波成分のみに対する暗号化を行うようにしたり、数サンプルおきに暗号化を行うようしたりすればよい。このようにしてデータ汚損度を制御すれば、適度に耳障りな再生

音を生成することが可能となる。

【００９２】

さて、次に、出力経路暗号化動作の詳細について説明する。

【００９３】

まず、本実施形態に係る情報処理装置１０１の概略動作について、図４を用いて説明する。

【００９４】

図４は、本実施形態に係る情報処理装置１０１の概略構成図である。

【００９５】

図４では、ＰＣなどの情報処理装置１０１のうち、表示に関する部分であって、かつ、出力経路暗号化動作に関する部分のみを示している。

【００９６】

図中、図３と同じ構成要素には同じ符号を付与してある。４０１は暗号処理部、４０２は復号処理部、４０３はデータドライバである。

【００９７】

ここでは、表示装置１０３は、例えば、液晶表示（ＬＣＤ：Liquid Crystal Display）装置や、デジタル／アナログ変換機能を具備したＣＲＴ（Cathode-Ray Tube）装置のような、デジタル入力の表示装置とする。

【００９８】

図４において、上述した配布経路暗号化動作によって表示制御装置３０３の内部に展開されたデジタルコンテンツを含む表示データ（平文表示データ）は、ＣＰＵ３０１の指示に従って、表示メモリ３０４に蓄積される。

【００９９】

表示制御装置３０３においては、暗号処理部４０１が、表示メモリ３０４に蓄積された平文表示データを入力し、入力した平文表示データの一部分に対して、表示制御装置３０３の内部に保持されている暗号鍵情報１０５を用いて暗号処理１０９を施し、表示制御装置３０３の内部に、暗号化された表示データを得る。得られた暗号化表示データは、表示制御装置３０３から表示装置１０３へ入力される。

【０１００】

続いて、表示装置１０３においては、復号処理部４０２が、入力した暗号化表示データ中の暗号化部分に対して、表示装置１０３の内部に保持されている暗号鍵情報１０５を用いて復号処理１１０を施し、表示装置１０３の内部に、平文表示データを得る。続いて、データドライバ４０３が、復号処理部４０２が復号した平文表示データを、表示画面上の各々の表示画素に供給することで、平文表示データの表示処理１１１を行う。

【０１０１】

以上の動作が出力経路暗号化動作に相当している。

【０１０２】

なお、暗号処理部４０２は、表示制御装置３０３内にハードウェアとして実装されるようにしてもよいし、また、表示制御装置３０３内に独自のＣＰＵおよびメモリを設け、ソフトウェアとして実装されるようにしてもよい。

【０１０３】

次に、本実施形態に係る表示制御装置３０３の概略動作について、図８を用いて説明する。

【０１０４】

図８は、本実施形態に係る表示制御装置３０３の概略構成図である。

【０１０５】

図８では、表示制御装置３０３のうち、出力経路暗号化動作に関する部分のみを示している。

【０１０６】

図中、８０１はメモリ制御部、８０２はタイミング生成部、８０３はタイミング信号、８０４はメモリ制御信号、８０５はメモリアドレス信号、３０４は表示メモリ、８０６はＬＣＤ制御部、８０７はＬＣＤ制御信号、８０８は平文表示データ、８０９はタイミング制御部、８１０はＬＣＤ表示データ、８１１はシリアル／パラレル変換回路（Ｓ／Ｐ回路）、８１２はＳ／Ｐ済ＬＣＤ表示データ、８１３は暗号化Ｓ／Ｐ済ＬＣＤ表示データ、８１４はパラレル／シリアル変換回路（Ｐ／Ｓ回路）、８１５は暗号化ＬＣＤ表示データ、８１６は遅延回路、８１７

は遅延済ＬＣＤ制御信号である。

【０１０７】

図８において、メモリ制御部８０１は、タイミング生成部８０２から送られてくるタイミング信号８０３を用いて、メモリ制御信号８０４およびメモリアドレス信号８０５を生成し、表示メモリ３０４から平文表示データ８０８を順次読み出す。

【０１０８】

一方、ＬＣＤ制御部８０６は、タイミング生成部８０２から送られてくるタイミング信号８０３を用いて、ＬＣＤの表示タイミングを制御するＬＣＤ制御信号８０７を生成する。

【０１０９】

タイミング制御部８１０は、表示メモリ３０４から読み出された平文表示データ８０８を、ＬＣＤ制御信号８０６による表示タイミングに合わせて、ＬＣＤ表示データ８１０として送り出す。

【０１１０】

すなわち、表示メモリ３０４から読み出された平文表示データ８０８は、タイミング制御部８０９によって、ＬＣＤ制御信号８０７に同期したＬＣＤ表示データ８１１となる。

【０１１１】

例えば、ＬＣＤ制御信号８０７が、１データ転送クロック同期で１画素分の表示データを転送し、かつ、１画素が１６ビットのデータから構成されているとすると、ＬＣＤ表示データ８１０は、１６ビットデータバスとなる。ここで、暗号処理に、例えば、ＤＥＳのようなブロック暗号を用いた場合、暗号処理部４０１は、暗号鍵情報１０５を用いて、６４ビット単位のブロック暗号処理を施すこととなる。

【０１１２】

両者の処理単位の違いを吸収するために、本実施形態に係る表示制御装置３０３においては、Ｓ／Ｐ回路８１１およびＰ／Ｓ回路８１５を用いている。Ｓ／Ｐ回路８１１は、ＬＣＤ表示データ８１０のデータ幅（ここでは、１６ビット単位

）を、暗号処理単位（ここでは、６４ビット単位）幅に変換し、Ｓ／Ｐ済ＬＣＤ表示データ８１２として暗号処理部４０１に供給するものであり、また、Ｐ／Ｓ回路８１５は、暗号処理部４０１によって暗号処理が施された後の暗号化Ｓ／Ｐ済ＬＣＤ表示データ８１３のデータ幅を、ＬＣＤ表示データ８１０のデータ幅に変換し、暗号化ＬＣＤ表示データ８１５としてデータドライバ４０３に供給するものである。

【０１１３】

ＬＣＤ表示データ８１０のデータ幅と暗号処理部４０１の暗号処理単位幅とに応じて、Ｓ／Ｐ回路８１１およびＰ／Ｓ回路８１４の構成は異なる。

【０１１４】

図８に示すように、本実施形態に係る表示制御装置３０３においては、Ｓ／Ｐ回路８１１，暗号処理部４０１，Ｐ／Ｓ回路８１４による処理が設けられているので、これらの処理による遅延と同等の遅延を、遅延回路８１６によって、ＬＣＤ制御部８０６が生成したＬＣＤ制御信号８０７に加え、遅延済ＬＣＤ制御信号８１７として出力するようにすることで、Ｐ／Ｓ回路８１４から出力される暗号化ＬＣＤ表示データ８１５が、遅延済ＬＣＤ制御信号８１７に同期してデータドライバ４０３に供給されるようにしている。

【０１１５】

これにより、表示制御装置３０３による表示タイミング制御の処理途上で、表示データの一部分に対して暗号処理を施すこと、すなわち、ＬＣＤ表示データ８１０のリアルタイム暗号処理による暗号化ＬＣＤ表示データ８１５の作成が可能となる。

【０１１６】

次に、本実施形態に係る表示装置１０３の概略動作について、図９を用いて説明する。

【０１１７】

図９は、本実施形態に係る表示装置１０３の概略構成図である。

【０１１８】

図９では、表示装置１０３が液晶表示装置である場合を例にしており、表示装

置１０３のうち、出力経路暗号化動作に関する部分（すなわち、データドライバ４０３に相当する液晶駆動ドレイン側ドライバ）のみを示している。

【０１１９】

図中、９０１は暗号化表示データの取り込み信号（ＣＬ２信号）、９０２は暗号化表示データ、９０３はＬＣＤ駆動電圧を出力するタイミング信号（ＣＬ１信号）、９０４はＬＣＤ駆動用電源、９０５は液晶駆動出力信号、９０６はラッチアドレスセレクタ、９０７はラッチ回路－１、９０８はラッチ回路－２、９０９は回路駆動電圧から液晶駆動電圧へ昇圧するレベルシフタ、９１０は液晶駆動用の電圧レベルを発生する液晶駆動回路、９１１はラッチ回路－３、９１２は平文表示データである。

【０１２０】

図９において、ラッチアドレスセレクタ９０６は、暗号化表示データ９０２の入力と同期して表示制御装置３０３から入力したＣＬ２信号９０１（図８に示した遅延済ＬＣＤ制御信号８１７に相当している。）の立下りをカウントすることで、ラッチ回路－１（９０７）に対するラッチ信号を生成する。

【０１２１】

表示制御装置３０３から入力した暗号化表示データ９０２は、ラッチアドレスセレクタ９０６が生成するラッチ信号によって、ラッチ回路－１（９０７）上に入力順に保持されていく。

【０１２２】

ＣＬ１信号９０３は、表示１ラインごとに入力する水平同期信号であり、ＣＬ１信号９０３の入力によって、ラッチ回路－１（９０７）上にラッチされた１表示ライン分の暗号化表示データ９０２は、１ライン表示期間ごとに、１ライン分ずつ、ラッチ回路－２（９０８）上にラッチされる。

【０１２３】

ラッチ回路－２（９０８）上にラッチされた１ライン分の暗号化表示データ９０２は、復号処理部４０２によって、暗号鍵情報１０５を用いた復号処理１００が施されて平文表示データ９１２となり、ＣＬ１信号９０３によって、１ライン表示期間ごとに、１ライン分ずつ、ラッチ回路－３（９１１）上にラッチされる

。

【０１２４】

ラッチ回路－３（９１１）上にラッチされた１ライン分の平文表示データ９１２は、レベルシフタ９０９および液晶駆動回路９１０を介して液晶駆動電圧に変換され、１ライン表示期間、液晶に印加される。

【０１２５】

以上の処理により、１ラインごとに液晶への表示動作が実行される。

【０１２６】

ここで、復号処理に、例えば、ＤＥＳのようなブロック暗号を用いた場合、復号処理部４０２は、ラッチ回路－２（９０８）から出力されるビット数を、同時に並列処理可能な分だけ、ブロック単位に並列させる。例えば、液晶駆動ドレイン側ドライバが、１ライン当たり１０２４画素構成で１画素当たり１８ビット出力であるとすると、１ライン当たり１８４３２ビットとなるので、６４ビット単位（ＤＥＳによる処理単位）のブロックを２８８個並列させる。そして、復号処理部４０２は、暗号鍵情報１０５を用いて、６４ビット単位のブロック復号処理を施すこととなる。

【０１２７】

これにより、表示装置１０３の液晶駆動ドレイン側ドライバによる表示制御の処理途上で、表示データの一部分に対して復号処理を施すこと、すなわち、暗号化表示データ９１２のリアルタイム復号処理による平文表示データ９１２の作成・表示が可能となる。

【０１２８】

なお、本実施形態に係る表示装置１０３は、図９に示す構成ではなく、図１０に示す構成にしてもよい。

【０１２９】

図１０は、本実施形態に係る表示装置１０３の他の概略構成図である。

【０１３０】

図１０でも、図９と同様に、表示装置１０３が液晶表示装置である場合を例にしており、表示装置１０３のうち、出力経路暗号化動作に関する部分（すなわち

、データドライバ４０３に相当する液晶駆動ドレイン側ドライバ）のみを示している。

【０１３１】

図中、図９と同じ構成要素には同じ符号を付与してある。１００１はＳ／Ｐ回路、１００２はＰ／Ｓ回路、１００３はＳ／Ｐ済表示データ、１００４は平文表示データである。

【０１３２】

図１０に示す表示装置１０３は、暗号化表示データ９０２のデータ幅が、１画素当たりのデータビット数とデータ転送クロック（ＣＬ２信号９０１）とに依存し、復号処理部４０２の復号処理単位のデータ幅と異なっている場合に、Ｓ／Ｐ回路１００１によって、暗号化表示データ９０２のデータ幅を適切な復号処理単位のデータ幅に変換し、Ｓ／Ｐ済表示データ１００３としてから、復号処理部４０２によって、暗号鍵情報１０５を用いて復号処理を行い、復号処理によって得られた平文表示データ１００４を、Ｐ／Ｓ回路１００２によって、平文表示データ９１２のデータ幅に変換するようにしたものである。

【０１３３】

復号処理部４０２は、最低１ブロックを処理できればよく、１画素当たりの暗号化表示データ９０２のビット数とＣＬ２信号９０１とに応じて、処理ブロックを並列させるようにしてもよい。

【０１３４】

以上、表示装置１０３が液晶表示装置である場合を例にとって、出力経路暗号化動作について説明したが、表示装置１０３が、例えば、デジタル入力でデジタル／アナログ変換部を具備するＣＲＴ装置である場合でも、デジタル処理を行う途上で、同様の復号処理を行うようにすれば、平文表示データの作成・表示が可能となる。

【０１３５】

次に、出力経路暗号化動作で、表示制御装置３０３から出力される表示データの暗号化方法の一例について、図１１および図１２を用いて説明する。

【０１３６】

図１１は、表示制御装置３０３から出力される表示データの暗号化方法の一例を示す説明図であり、暗号化された表示データを表示装置１０３で表示した場合の表示イメージを示す説明図である。

【０１３７】

図１１では、元画像（本来の平文表示データ）の暗号化方法として、ライン方向に暗号処理を施す暗号化方法と、カラム方向に暗号処理を施す暗号化方法とを示している。

【０１３８】

（１）ライン方向に暗号処理を施す暗号化方法

例えば、図１１（ａ）に示す元画像（本来の平文表示データ）に対して、本方法による暗号化を行う際には、ライン方向に、複数ライン分（例えば、数ライン程度）の表示データを１単位とし、これらの単位の一部の単位を暗号処理の処理対象として、暗号処理を施すようにする。具体的には、数ライン分の表示データごとに、交互に、暗号処理を施す場合と暗号処理を施さない場合とを繰り返すようにする。

【０１３９】

本方法により暗号化された表示データは、暗号鍵情報１０５を用いた復号処理を施せば、表示装置１０３に表示される際のイメージは、図１１（ａ）に示す元画像と同じイメージになるが、暗号鍵情報１０５を用いた復号処理を施さなければ、表示装置１０３に表示される際のイメージは、図１１（ｂ）に示すように、数ラインおきに数ライン分が汚損された表示データとなる。

【０１４０】

本方法では、１単位とするライン数を予め決定しておき、決定したライン数ごとに、表示制御装置３０３の暗号処理部４０１が選択的に暗号化すると共に、表示装置１０３の復号処理部４０２が選択的に復号するようにする。これにより、表示データの一部に対する汚損が可能となり、また、表示制御装置３０３の暗号処理部４０１および表示装置１０３の復号処理部４０２における暗号／復号処理量の削減が可能となる。

【０１４１】

また、１単位とするライン数を増減させることで、表示データの汚損度合を制御可能であり、どの程度の開示を行うかを自由に変更することができる。

【０１４２】

（２）カラム方向に暗号処理を施す暗号化方法

例えば、図１１（ａ）に示す元画像（本来の平文表示データ）に対して、本方法による暗号化を行う際には、カラム方向に、複数カラム分（例えば、数カラム程度）の表示データを１単位とし、これらの単位の一部の単位を暗号処理の処理対象として、暗号処理を施すようにする。具体的には、数カラム分の表示データごとに、交互に、暗号処理を施す場合と暗号処理を施さない場合とを繰り返すようにする。

【０１４３】

本方法により暗号化された表示データは、暗号鍵情報１０５を用いた復号処理を施せば、表示装置１０３に表示される際のイメージは、図１１（ａ）に示す元画像と同じイメージになるが、暗号鍵情報１０５を用いた復号処理を施さなければ、表示装置１０３に表示される際のイメージは、図１１（ｃ）に示すように、数カラムおきに数カラム分が汚損された表示データとなる。

【０１４４】

本方法では、１単位とするカラム数を予め決定しておき、決定したカラム数ごとに、表示制御装置３０３の暗号処理部４０１が選択的に暗号化すると共に、表示装置１０３の復号処理部４０２が選択的に復号するようにする。これにより、表示データの一部に対する汚損が可能となり、また、表示制御装置３０３の暗号処理部４０１および表示装置１０３の復号処理部４０２における暗号／復号処理量の削減が可能となる。

【０１４５】

また、１単位とするカラム数を増減させることで、表示データの汚損度合を制御可能であり、どの程度の開示を行うかを自由に変更することができる。

【０１４６】

図１２は、表示制御装置３０３から出力される表示データの暗号化方法の一例を示す説明図であり、図１２では、元画像（本来の平文表示データ）中の１画素

分の表示データについて、その一部分に対して暗号処理を施す暗号化方法を示している。

【０１４７】

本方法では、１画素内の表示データ中の上位ビットのみに暗号処理を施すようにするか、または、１画素内の表示データ中の下位ビットのみに暗号処理を施すようにする。

【０１４８】

上位ビットのみを暗号化し、下位ビットは平文のままとした場合は、表示データの変化量が大きくなる。そこで、暗号化表示データを復号せずに表示装置１０３上で表示すると、データの汚損度が大きく、表示データの観察は困難となる。

【０１４９】

また、下位ビットのみを暗号化し、上位ビットは平文のままとした場合は、表示データの変化量は少ない。そこで、暗号化表示データを復号せずに表示装置１０３上で表示すると、データの汚損度が小さく、画面上のちらつきとして観察されるが、表示データのおおまかな観察は可能である。

【０１５０】

図１２では、１画素分の表示データが８ビットで構成され、ある平文表示データが「５５ｈ」であるとしたときに、上位ビットのみを暗号化して「５５ｈ」が「ｅ５ｈ」になり、下位ビットのみを暗号化して「５５ｈ」が「５２ｈ」になった例を示した。このように、上位ビットのみを暗号化する方が、平文表示データからの変化量が大きくなるので、より異なった表示内容として観測されることとなる。

【０１５１】

本方法では、上位ビットのみを暗号化するか、または、下位ビットのみを暗号化するかを選択することで、表示データの汚損度合を選択することが可能であり、また、表示制御装置３０３の暗号処理部４０１および表示装置１０３の復号処理部４０２における暗号／復号処理量の削減が可能となる。

【０１５２】

以上、ライン方向／カラム方向に暗号処理を施す暗号化方法、および、１画素

内の表示データ中の上位ビット／下位ビットのみに暗号処理を施す暗号化方法について説明したが、これらの方法を任意に組み合わせるようにしてもよい。

【０１５３】

本実施形態に係るデジタルコンテンツ配布システムによれば、出力経路暗号化動作によって、従来は行われていなかった、最終出力装置である表示装置１０３への出力経路でのデジタルコンテンツの著作権保護が可能となる。

【０１５４】

そして、本実施形態に係るデジタルコンテンツ配布システムによれば、出力経路暗号化動作において、デジタルコンテンツ（表示データ）を単純に暗号化するのではなく、暗号処理の処理対象とするデータを選択し、一部分のみを暗号化するようにしているので、正当な暗号鍵情報１０５を有していない場合には、元画像の一部分が汚損した状態となる。一部分が汚損されたデジタルコンテンツは、その価値が損なわれるので、デジタルコンテンツの不正コピーを防止することが可能となり、また、デジタルコンテンツの一部分が開示されるので、ユーザの視聴要求を刺激し、デジタルコンテンツの完全な視聴を促すことが可能となる。

【０１５５】

さらに、本実施形態に係るデジタルコンテンツ配布システムによれば、出力経路暗号化動作において、デジタルコンテンツの一部分だけを暗号処理の処理対象とし、デジタルコンテンツ全体に対する暗号処理を避けることによって、暗号処理／復号処理の処理量の軽減も可能となっている。なお、汚損度と処理量とはトレードオフの関係にあり、要求に応じて優先度の変更が容易に可能である。

【０１５６】

以上説明したように、本実施形態に係るデジタルコンテンツ配布システムによれば、出力経路暗号化動作によって、デジタルコンテンツの出力経路上で著作権を保護しつつ、ユーザの視聴欲求を刺激することが可能となる。

【０１５７】

なお、本実施形態に係る情報処理装置１０１は、図４に示す構成ではなく、図１３に示す構成にし、図４に示した暗号処理部４０１を、ソフトウェアで実現するようにしてもよい。

【０１５８】

図１３は、本実施形態に係る情報処理装置１０１の他の概略構成図である。

【０１５９】

図１３でも、図４と同様に、ＰＣなどの情報処理装置１０１のうち、表示に関する部分であって、かつ、出力経路暗号化動作に関する部分のみを示している。

【０１６０】

図中、図４と同じ構成要素には同じ符号を付与してある。７０１は不揮発性記憶装置である。

【０１６１】

図１３に示す構成の情報処理装置１０１においては、図４に示した暗号処理部４０１の動作を、ＣＰＵ３０１がシステムメモリ３０２上にプログラムをロードして実行することで実現するものである。すなわち、図１３に示す構成の情報処理装置１０１は、表示制御装置３０３ではなく、ＣＰＵ３０１が表示データを暗号化するようにしている。

【０１６２】

図１４は、図１３に示す構成の情報処理装置１０１の概略動作を示す説明図である。

【０１６３】

図１４に示すように、表示メモリ３０４に蓄積された平文表示データ８０８は、ＣＰＵ３０１の指示に従って、表示制御装置３０３およびバス３０７を介してシステムメモリ３０２に入力される。

【０１６４】

ＣＰＵ３０１は、入力した平文表示データ８０８に対して、暗号鍵情報１０５を用いて暗号処理１０９を施す。ＣＰＵ３０１によって暗号化された暗号化表示データ９０２は、バス３０７および表示制御装置３０３を介して表示メモリ３０４にに入力される。表示メモリ３０４に蓄積された暗号化表示データ９０２は、表示制御装置３０３によって読み出され、表示装置１０３に出力される。

【０１６５】

すなわち、図１３に示す構成の情報処理装置１０１においては、ＣＰＵ３０１

が、表示メモリ３０４上に平文表示データ８０８を生成し、さらに、平文表示データ８０８から表示メモリ３０４上に暗号化表示データ９０２を生成する。表示制御装置３０３は、暗号化表示データ９０２の読み出し動作を行い、表示動作を行う。

【０１６６】

ここで、暗号鍵情報１０５は、図４を用いた説明では、表示制御装置３０３の内部に保持されているものとしたが、図１３に示す構成の情報処理装置１０１においては、暗号鍵情報１０５は、不揮発性記憶装置７０１に保持されているものとする。

【０１６７】

また、本実施形態に係る情報処理装置１０１は、図４および図１３のいずれにおいても、情報処理装置１０２本体と表示装置１０３とを備えた構成としているが、配布経路暗号化動作で説明したのと同様に、情報処理装置本体１０２と表示装置１０３が一体化した構成であってもよい。すなわち、本実施形態に係る情報処理装置１０１を、いわゆるＰＤＡなどと呼ばれる携帯情報端末としてもよい。

【０１６８】

上述したように、一般に、携帯情報端末は、比較的性能の低いＣＰＵや小容量のメモリなどを用いて構成されることが多いので、比較的重い処理である暗号処理は携帯情報端末にとって大きな負担になるという問題がある。

【０１６９】

そこで、このような問題がある携帯情報端末を、本実施形態に係るデジタルコンテンツ配布システムで用いるようにすれば、全体ではなく一部分が暗号化されたデジタルコンテンツを扱うことにより、本発明が目的とする、著作権保護とユーザの視聴覚欲求刺激の両立を実現することができる上、暗号処理量の低減による負荷低下効果を得ることができる。特に、携帯情報端末が暗号処理をソフトウェアで実現する場合には、暗号処理用に高性能なＣＰＵや大容量メモリを搭載する必要がなくなり、低コスト化，低消費電力化といった効果が得られる。また、携帯情報端末が暗号処理専用のハードウェアを備えるようにする場合には、暗号処理専用のハードウェアに必要な処理速度が低下することから、低動作速度によ

る低消費電力化，ハードウェア論理の小規模化による低コスト化といった効果が得られる。

【０１７０】

ところで、上述の説明では、デジタル表示装置への出力を例にしたが、必ずしも表示のみを対象としている訳ではない。

【０１７１】

例えば、デジタル入力を持った音声出力装置においても、ＰＣＭ（Pulse Code Modulation）符号化された音声データに対して、同様に、数サンプルおきに暗号化を施すことで、出力装置経路暗号化動作を実現することが可能である。

【０１７２】

以上説明したように、本実施形態に係るデジタルコンテンツ配布システムは、デジタルコンテンツのフォーマットに依存する形で、デジタルコンテンツの一部分に対して暗号処理を施すようにすることで、正当な暗号鍵情報を有さない場合に、一部が汚損されたデジタルコンテンツとなるようにしている。そこで、デジタルコンテンツの著作権を保護しつつ、ユーザの視聴覚欲求を刺激することが可能となる。

【０１７３】

従って、本実施形態に係るデジタルコンテンツ配布システムによれば、付加価値の高いデジタルコンテンツを、安全に半導体記憶媒体やデジタルネットワーク上で流通させることが可能となり、デジタルコンテンツ配布サービスなどへの応用が可能となる。

【０１７４】

なお、デジタルコンテンツの保護においては、配布経路暗号化動作および出力経路暗号化動作のうちのいずれか一方を用いたシステムとしてもよいし、また、両者を組み合わせ、２つの独立した暗号方式によって、デジタルコンテンツの保護を行うシステムとしてもよい。

【０１７５】

【発明の効果】

以上説明したように、本発明によれば、デジタルコンテンツの著作権を保護し

つつ、ユーザの視聴覚欲求を刺激することの可能な、デジタルコンテンツの配布が可能となる。

【図面の簡単な説明】

【図１】本実施形態に係るデジタルコンテンツ配布システムの概略構成図。

【図２】本実施形態に係るデジタルコンテンツ配布システムの概略動作フローチャート。

【図３】本実施形態に係る情報処理装置の概略構成図。

【図４】本実施形態に係る情報処理装置の概略構成図。

【図５】デジタルコンテンツ配布装置から配布されるデジタルコンテンツの暗号化方法の一例を示す説明図。

【図６】図５に示す暗号化方法で暗号化されたデジタルコンテンツを表示装置で表示した場合の表示イメージを示す説明図。

【図７】本実施形態に係る情報処理装置の概略構成図。

【図８】本実施形態に係る表示制御装置の概略構成図。

【図９】本実施形態に係る表示装置の概略構成図。

【図１０】本実施形態に係る表示装置の概略構成図。

【図１１】表示制御装置から出力される表示データの暗号化方法の一例を示す説明図。

【図１２】表示制御装置から出力される表示データの暗号化方法の一例を示す説明図。

【図１３】本実施形態に係る情報処理装置の概略構成図。

【図１４】図１３に示した情報処理装置の概略動作を示す説明図。

【符号の説明】

１００：デジタルコンテンツ配布装置

１０１：情報処理装置

１０２：情報処理装置本体

１０３：表示装置

１０４：暗号鍵情報

１０５：暗号鍵情報

１０６：復号処理

１０７：コンテンツ展開処理

１０８：表示制御処理

１０９：暗号処理

１１０：復号処理

１１１：表示処理

３０１：中央演算装置（ＣＰＵ：Central Processing Unit）

３０２：システムメモリ

３０３：表示制御装置

３０４：表示メモリ

３０５：入力制御装置

３０６：通信制御装置

３０７：バス

３０８：復号処理部

３０９：コンテンツ展開処理部

４０１：暗号処理部

４０２：復号処理部

４０３：データドライバ

７０１：不揮発性記憶装置

８０１：メモリ制御部

８０２：タイミング生成部

８０３：タイミング信号

８０４：メモリ制御信号

８０５：メモリアドレス信号

８０６：ＬＣＤ（Liquid Crystal Display）制御部

８０７：ＬＣＤ制御信号

８０８：平文表示データ

８０９：タイミング制御部

８１０：ＬＣＤ表示データ

８１１：シリアル／パラレル変換回路（Ｓ／Ｐ回路）

８１２：Ｓ／Ｐ済ＬＣＤ表示データ

８１３：暗号化Ｓ／Ｐ済ＬＣＤ表示データ

８１４：パラレル／シリアル変換回路（Ｐ／Ｓ回路）

８１５：暗号化ＬＣＤ表示データ

８１６：遅延回路

８１７：遅延済ＬＣＤ制御信号

９０１：ＣＬ２信号

９０２：暗号化表示データ

９０３：ＣＬ１信号

９０４：ＬＣＤ駆動用電源

９０５：液晶駆動出力信号

９０６：ラッチアドレスセレクタ

９０７：ラッチ回路－１

９０８：ラッチ回路－２

９０９：レベルシフタ

９１０：液晶駆動回路

９１１：ラッチ回路－３

９１２：平文表示データ

１００１：Ｓ／Ｐ回路

１００２：Ｐ／Ｓ回路

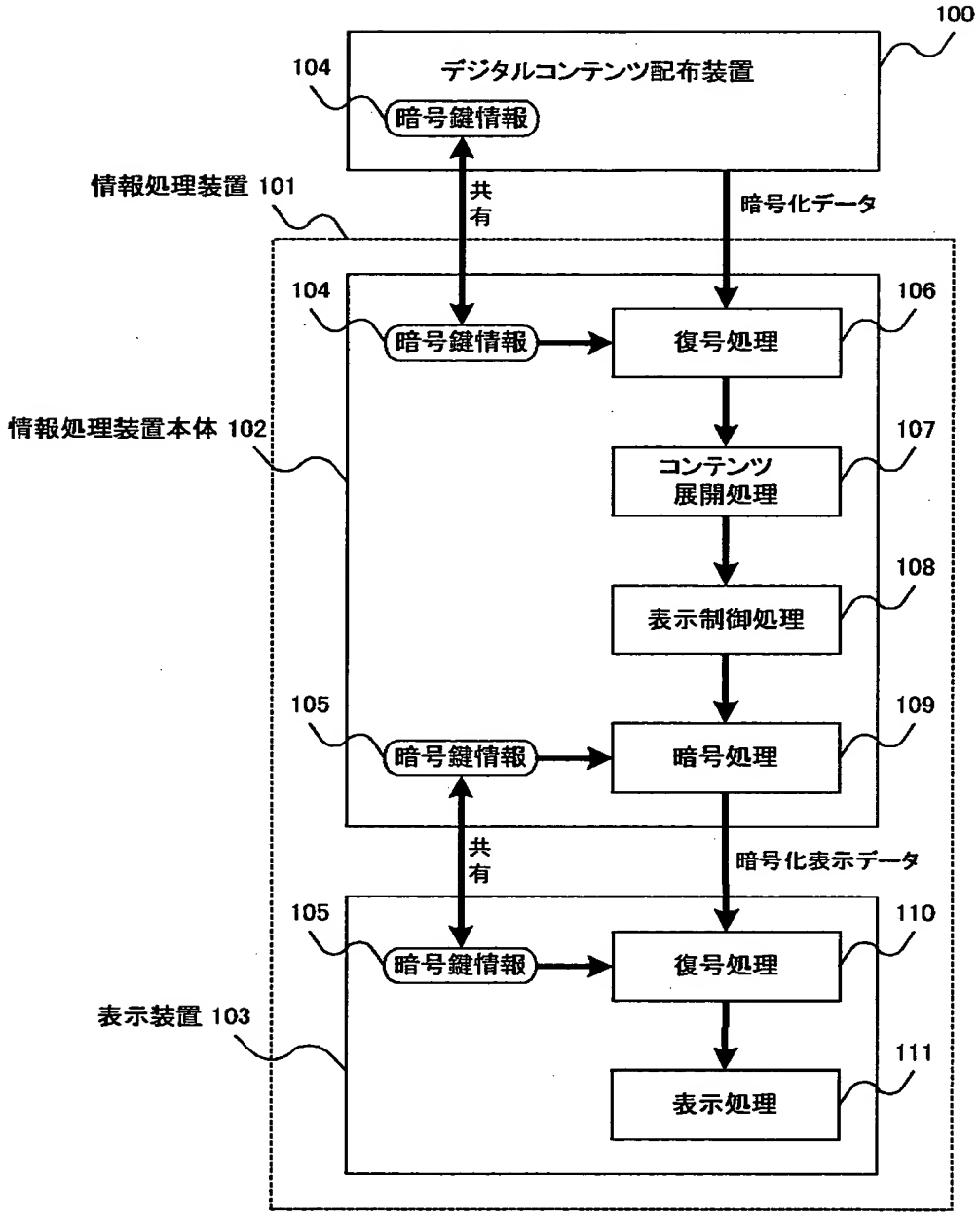
１００３：Ｓ／Ｐ済表示データ

１００４：平文表示データ

【書類名】図面

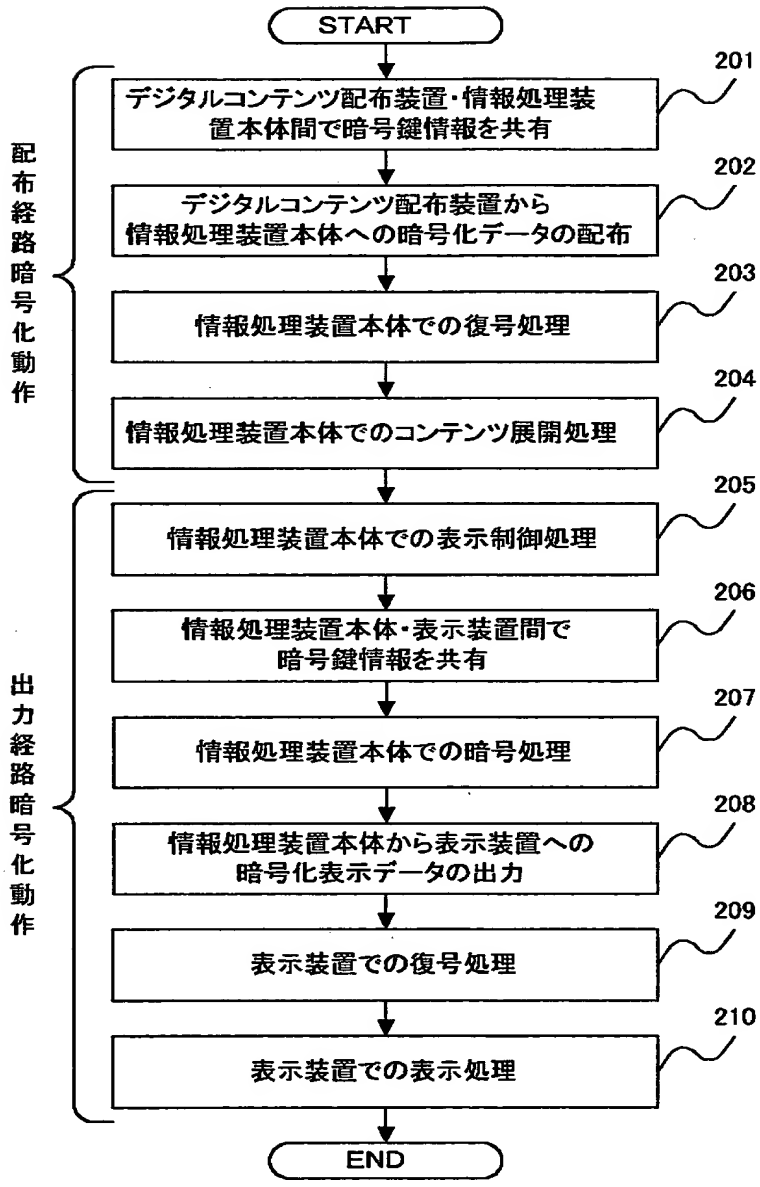
【図１】

図 1


100
デジタルコンテンツ配布装置
104
暗号鍵情報
情報処理装置 101
共有
暗号化データ
104
暗号鍵情報
106
復号処理
情報処理装置本体 102
107
コンテンツ展開処理
108
表示制御処理
105
暗号鍵情報
109
暗号処理
共有
暗号化表示データ
105
暗号鍵情報
110
復号処理
表示装置 103
111
表示処理

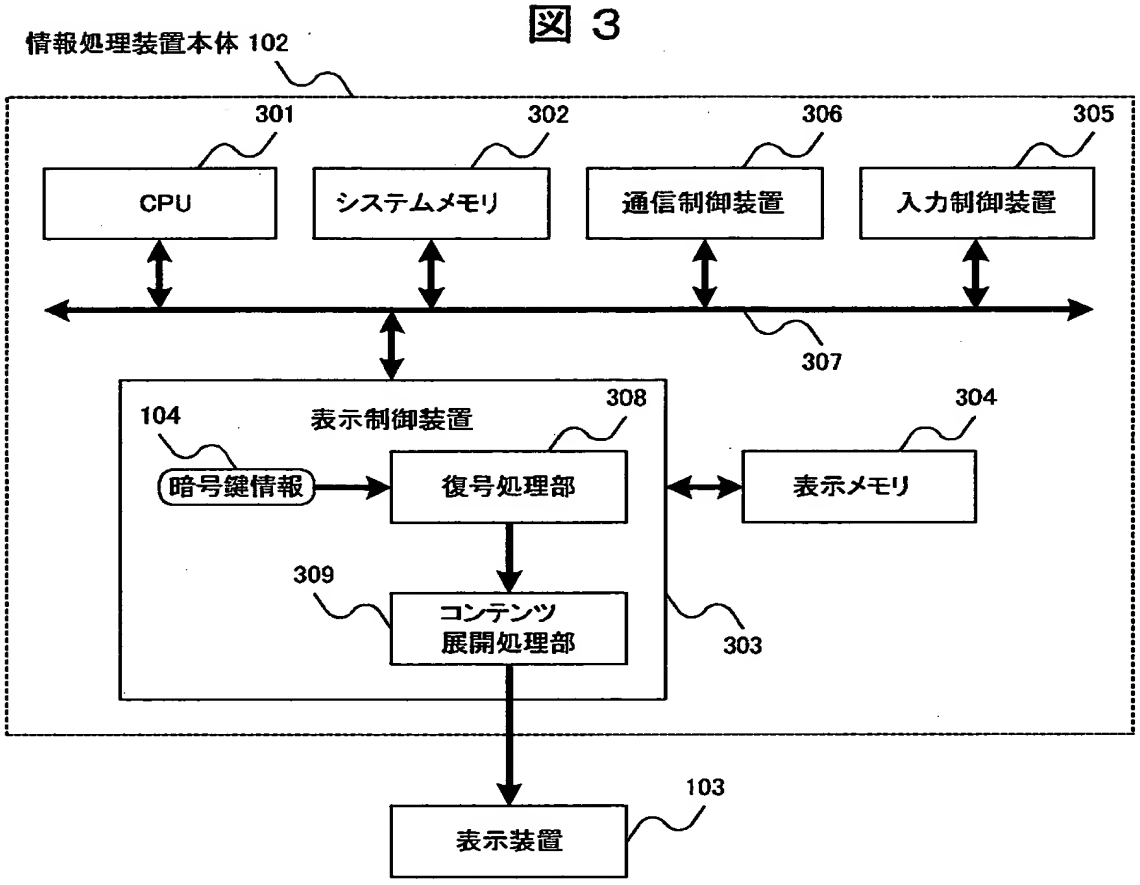
【図２】

図２


START
デジタルコンテンツ配布装置・情報処理装置本体間で暗号鍵情報を共有
201
デジタルコンテンツ配布装置から情報処理装置本体への暗号化データの配布
202
情報処理装置本体での復号処理
203
情報処理装置本体でのコンテンツ展開処理
204
配布経路暗号化動作
情報処理装置本体での表示制御処理
205
情報処理装置本体・表示装置間で暗号鍵情報を共有
206
情報処理装置本体での暗号処理
207
情報処理装置本体から表示装置への暗号化表示データの出力
208
表示装置での復号処理
209
表示装置での表示処理
210
出力経路暗号化動作
END

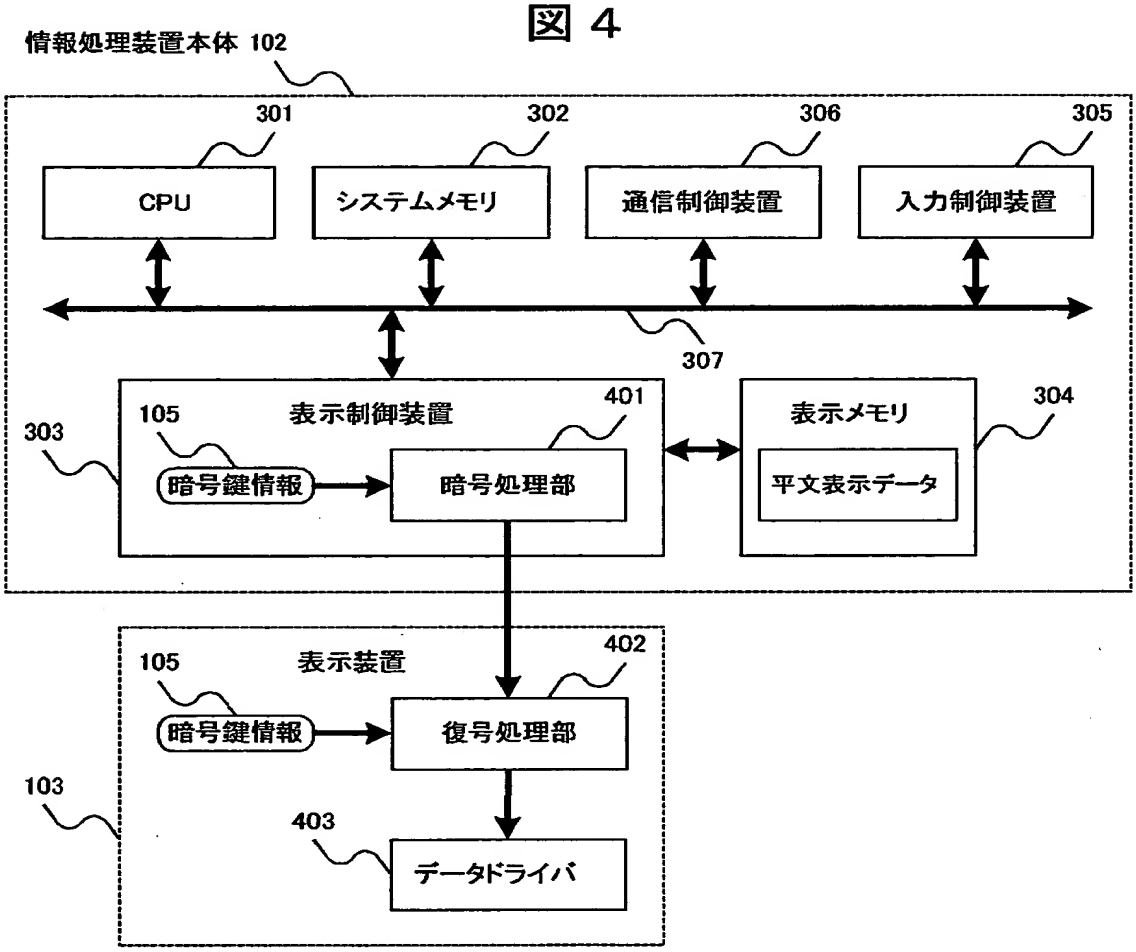
【図３】

図３


情報処理装置本体 102
301
CPU
302
システムメモリ
306
通信制御装置
305
入力制御装置
307
104
暗号鍵情報
表示制御装置
308
復号処理部
304
表示メモリ
309
コンテンツ
展開処理部
303
103
表示装置

【図４】

図４



【図５】

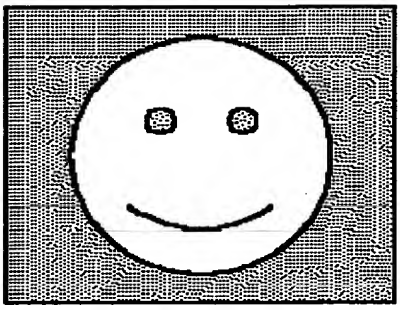
図５

暗号化対象	暗号鍵情報なしに得られるピクチャデータ			符号割り当て量@ピクチャデータ	暗号処理量@ピクチャデータ
	I	P	B		
Iピクチャデータ	×	×	×	大	大
Pピクチャデータ	○	×	×	中	中
Bピクチャデータ	○	○	×	小	小

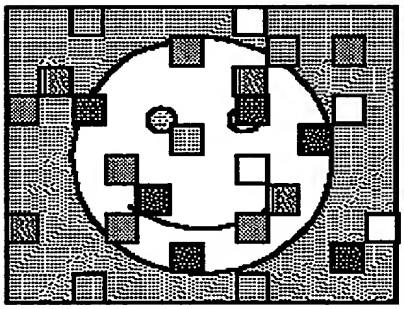
【図６】

図6

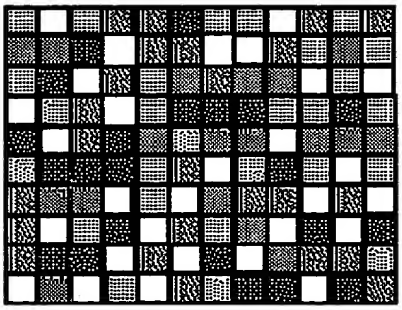
(a)



(b)

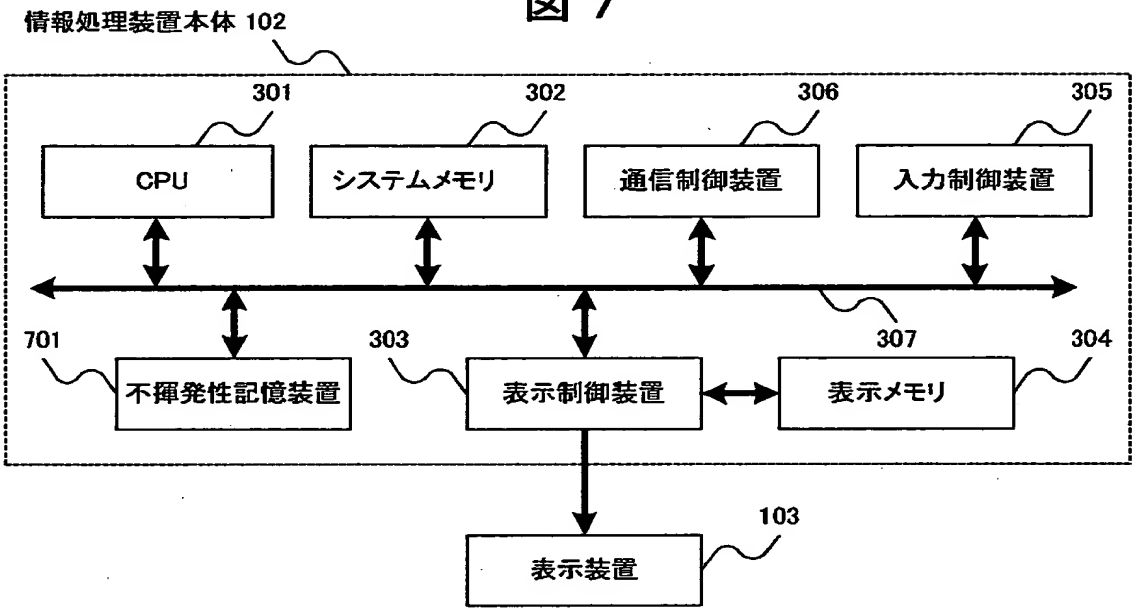


(c)



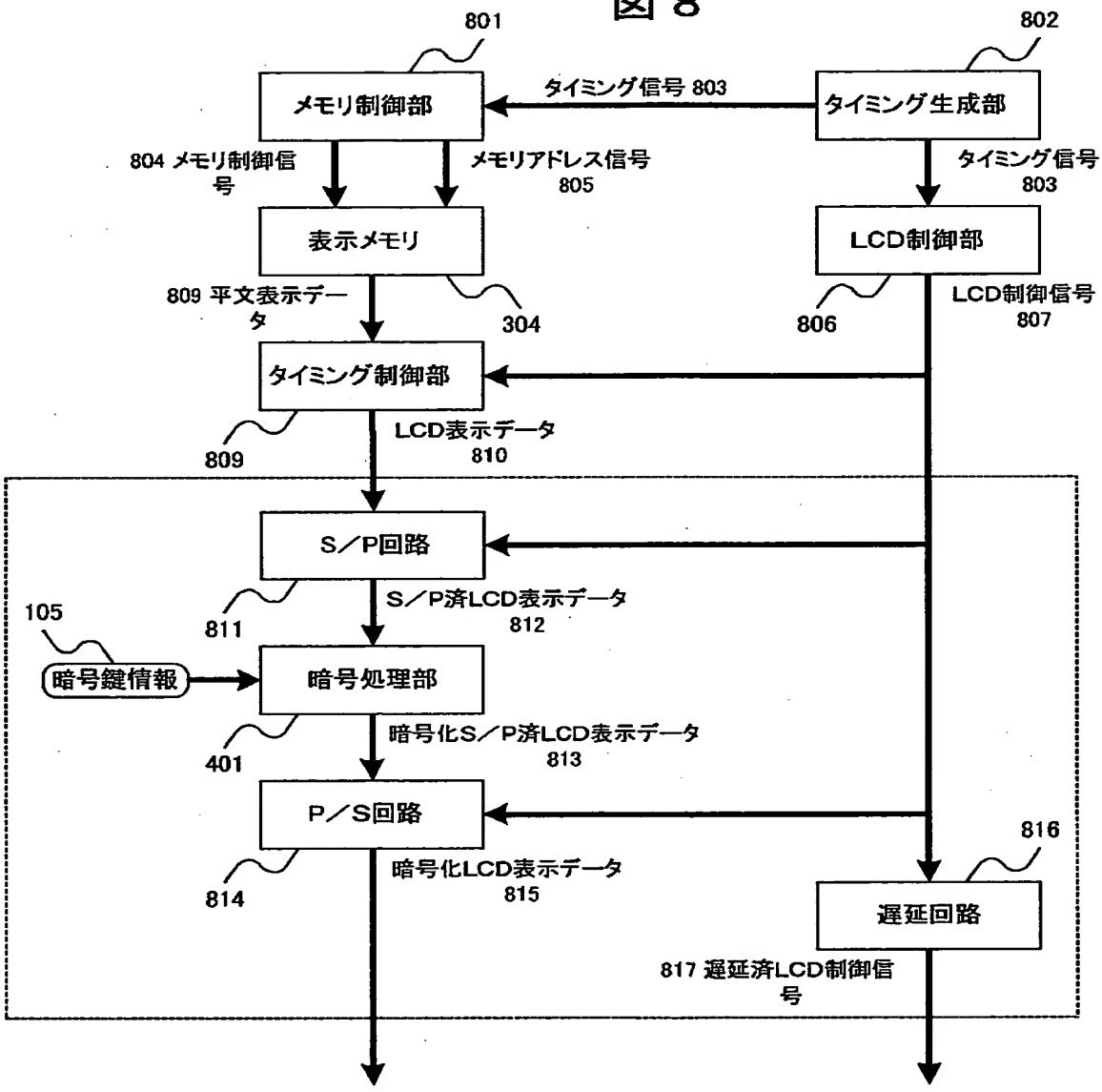
【図７】

図７


情報処理装置本体 102
301
302
306
305
CPU
システムメモリ
通信制御装置
入力制御装置
701
303
307
304
不揮発性記憶装置
表示制御装置
表示メモリ
103
表示装置

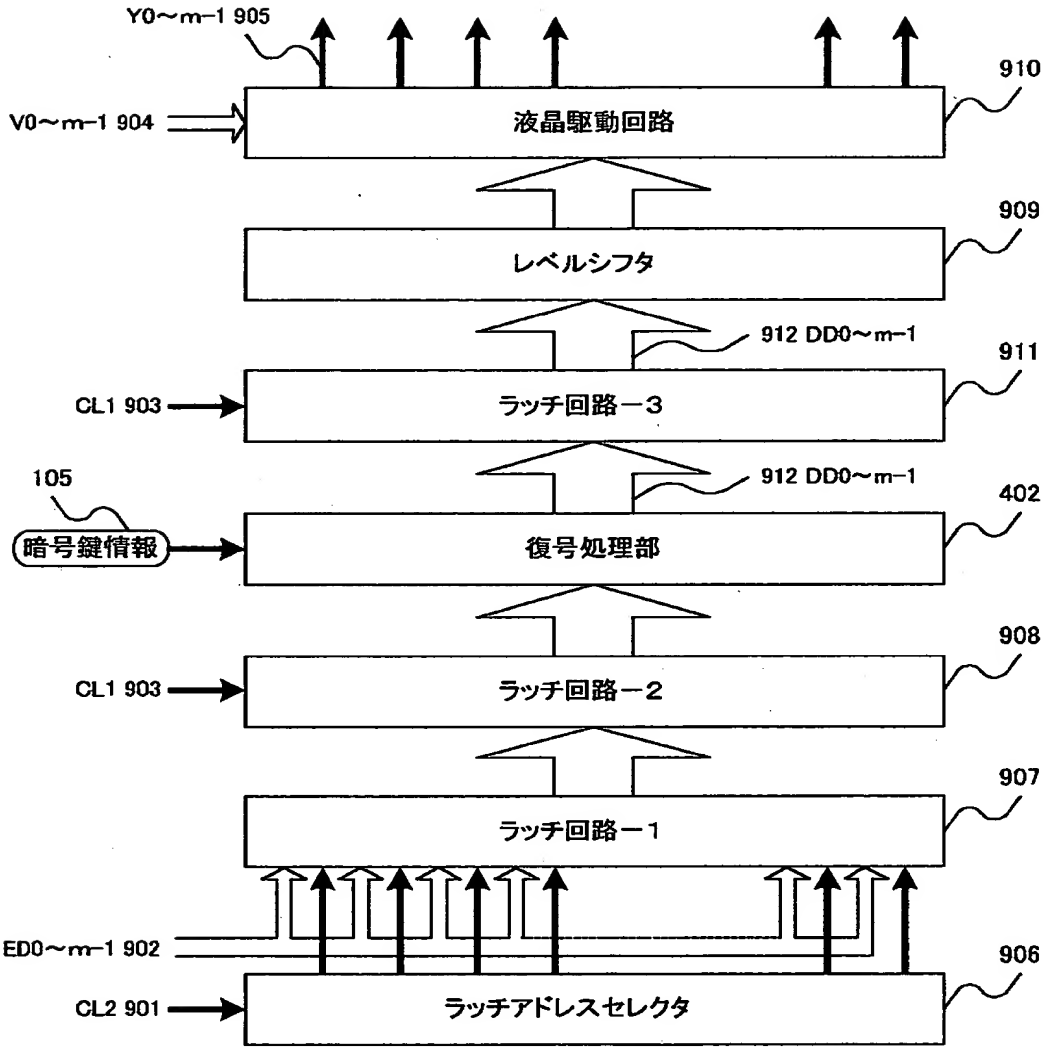
【図８】

図８


801
802
メモリ制御部
タイミング信号 803
タイミング生成部
804 メモリ制御信号
メモリアドレス信号 805
タイミング信号 803
表示メモリ
LCD制御部
809 平文表示データ
304
806
LCD制御信号 807
タイミング制御部
809
LCD表示データ 810
S／P回路
811
S／P済LCD表示データ 812
105
暗号鍵情報
暗号処理部
401
暗号化S／P済LCD表示データ 813
P／S回路
814
暗号化LCD表示データ 815
816
遅延回路
817 遅延済LCD制御信号

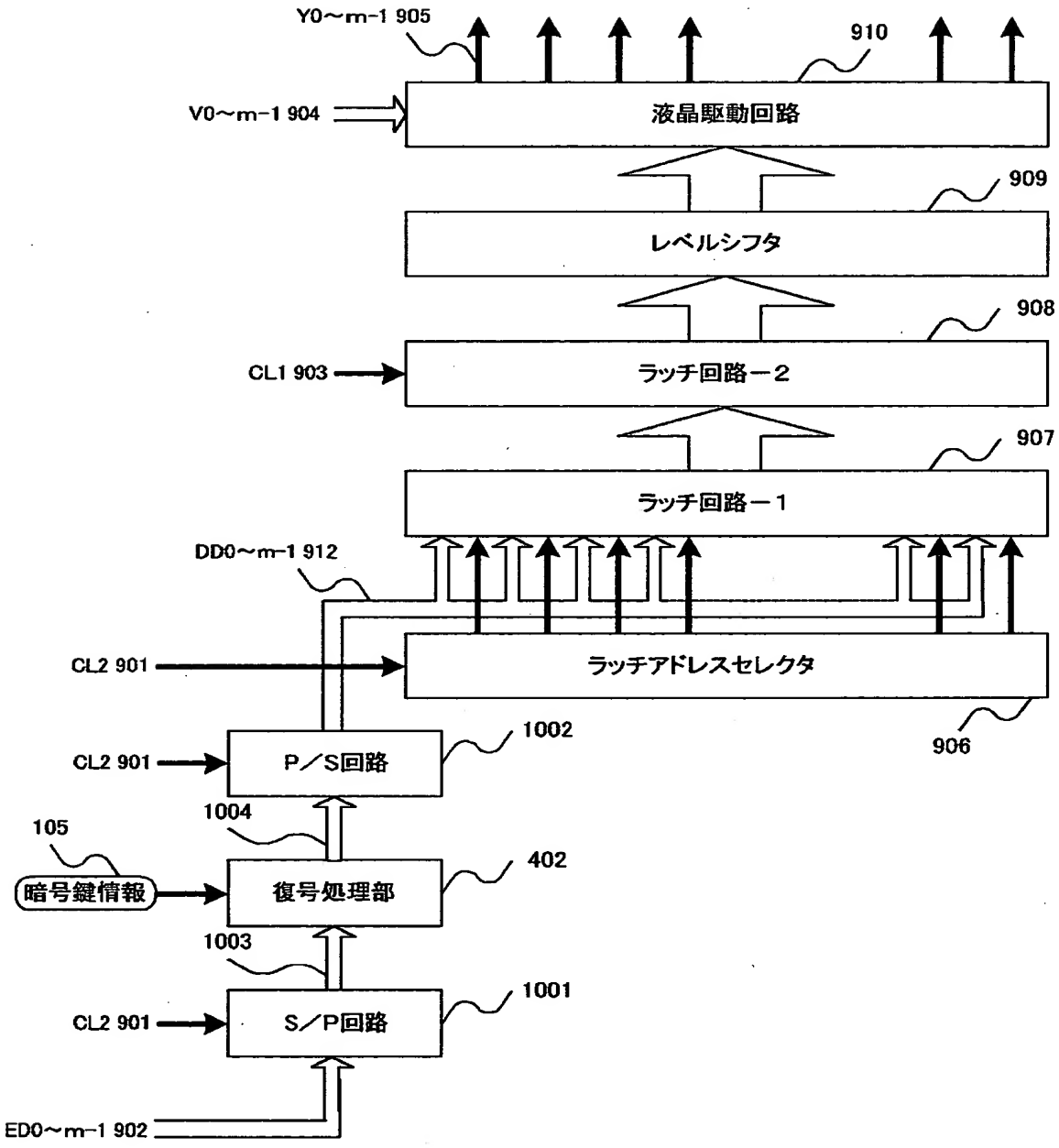
【図９】

図９


Y0～m-1 905
910
V0～m-1 904
液晶駆動回路
909
レベルシフタ
912 DD0～m-1
911
CL1 903
ラッチ回路－３
105
912 DD0～m-1
402
暗号鍵情報
復号処理部
908
CL1 903
ラッチ回路－２
907
ラッチ回路－１
ED0～m-1 902
906
CL2 901
ラッチアドレスセレクタ

【図１０】

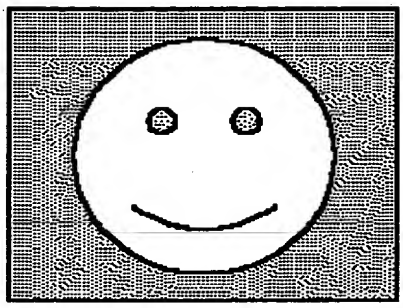
図 10


Y0～m-1 905
910
V0～m-1 904
液晶駆動回路
909
レベルシフタ
908
CL1 903
ラッチ回路－2
907
ラッチ回路－1
DD0～m-1 912
CL2 901
ラッチアドレスセレクタ
906
CL2 901
P／S回路
1002
1004
105
暗号鍵情報
復号処理部
402
1003
CL2 901
S／P回路
1001
ED0～m-1 902

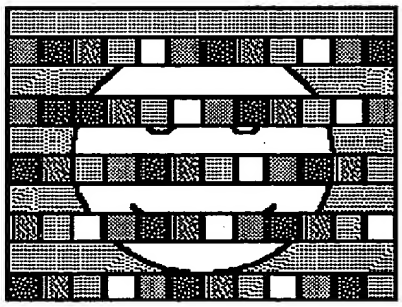
【図１１】

図11

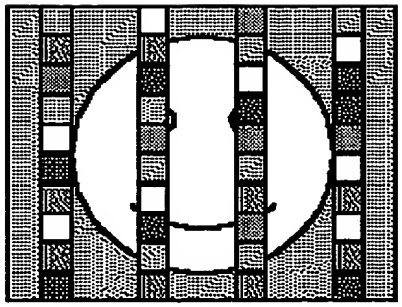
(a)



(b)



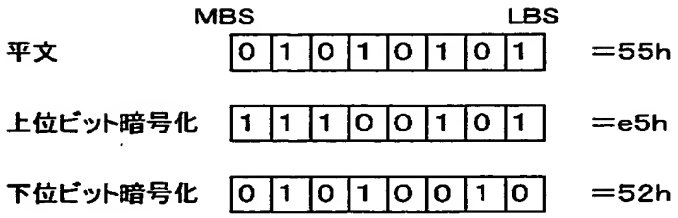
(c)



出証特２００１－３０９８６８４

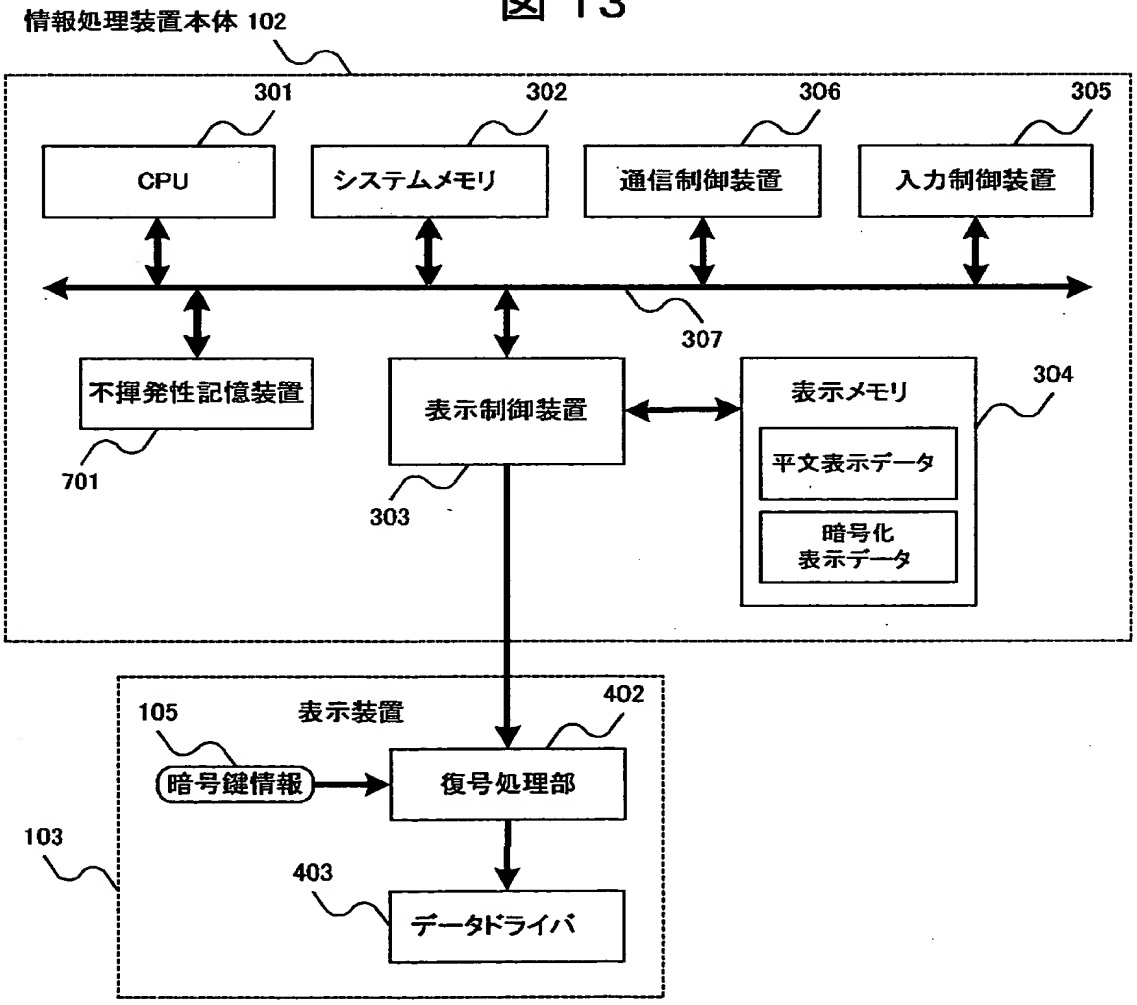
【図１２】

図 12



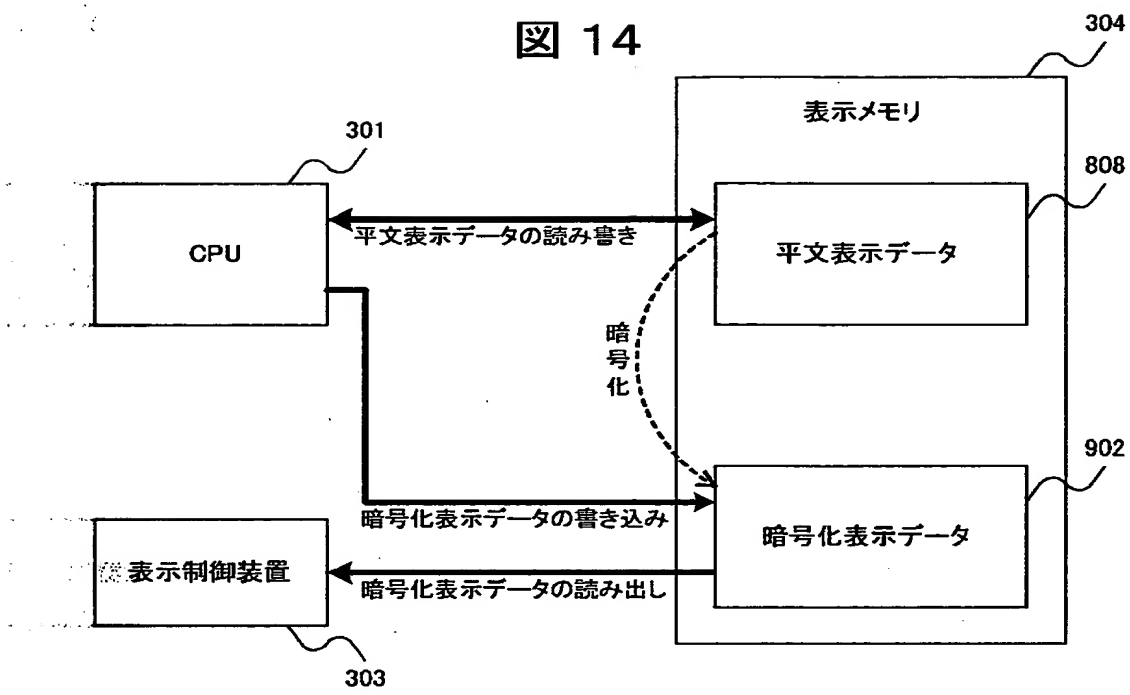
【図１３】

図 13



【図１４】

図 14



出証特２００１－３０９８６８４

【書類名】要約書

【課題】デジタルコンテンツの権利を保護しつつ、ユーザの視聴覚欲求を刺激する形でのデジタルコンテンツ配布を可能とする。

【解決手段】デジタルコンテンツ配布装置１００が、情報処理装置本体１０２と共有する暗号鍵情報１０４を用いて一部分が暗号化されたデジタルコンテンツを、情報処理装置本体１０２に配布し、情報処理装置本体１０２が、デジタルコンテンツ配布装置１００から配布されるデジタルコンテンツ中の暗号化部分に対して、暗号鍵情報１０４を用いて復号処理を施すようにしている。ここで、デジタルコンテンツ配布装置１００から配布されるデジタルコンテンツは、平文時のデジタルコンテンツのフォーマッティング単位を１単位とし、これらの単位中の一部の単位が暗号化対象となるようにして暗号化されたものである。

【選択図】図１

出証特２００１－３０９８６８４

出　願　人　履　歴　情　報

識別番号　　〔０００００５１０８〕

１．変更年月日　　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所